Polycom® RMX™ 1800 Administrator's Guide

Trademark Information

POLYCOM® and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Product model: Polycom® RMX™ 1800

> This software has not achieved UC APL certification.

This document provides the latest information for security-conscious users running Version 8.1 software. The information in this document is not intended to imply that DoD or DISA certifies Polycom RMX systems.

> For regulatory notices see the Polycom® RMX™ 1800 Hardware Guide.

End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom® RealPresence® Collaboration Server (RMX®) 1800 system end-user license agreements (EULA).

The EULA for your version is available on the Polycom Support page for the Polycom® RealPresence® Collaboration Server (RMX®) 1800 system.

Table of Contents

Polycom RMX 1800 Overview

About the Polycom RMX 1800 Administrator's Guide

The product names, *Polycom® RealPresence® Collaboration Server 1800* and *RMX® 1800* are used interchangeably throughout this Guide.

The *Polycom® RMX 1800 Administrator's Guide* provides instructions for configuring, deploying, and administering Polycom Multipoint Control Units (MCUs) for video conferencing. This guide will help you understand the Polycom video conferencing components, and provides descriptions of all available conferencing features. This guide will help you perform the following tasks:

*   Customize the Collaboration Server conferencing entities such as conference Profiles, IVR Services, Meeting Rooms, Entry Queues, etc., to your organization's needs.
*   Define Collaboration Server Users.
*   Advanced conference Management
*   Define Video Protocols and Resolution Configuration for CP Conferencing
*   Configure Templates, the Address Book and schedule Reservations.
*   Record Conferences
*   Configure the Collaboration Server to support special call flows and conferencing requirements, such as Cascading Conferences.
*   Configure the Collaboration Server for special applications and needs by setting various system flags.
*   Manage and troubleshoot the Collaboration Server's performance.

The *Polycom RMX 1800 Getting Started Guide* provides description of basic conferencing operations. It will help you perform the following tasks:

*   Unpack the Collaboration Server system and install it on a rack.
*   Connect the required cables to the Collaboration Server.
*   Perform basic configuration procedures.
*   Start a new conference and connect participants/endpoints to it.
*   Monitor ongoing conferences
*   Perform basic operations and monitoring tasks

Who Should Read This Guide?

System administrators and network engineers should read this guide to learn how to properly set up Polycom Collaboration Server systems. This guide describes administration-level tasks.

For detailed description of first time installation and configuration, description of the *Collaboration Server Web Client,* and basic operation of your Collaboration Server system, see the *Polycom RMX 1800 Getting Started Guide*.

Prerequisites

This guide assumes the user has the following knowledge:

*   Familiarity with Windows® XP or Windows 7 operating systems and interface.
*   Familiarity with Microsoft® Internet Explorer® Version 7, 8 or 9.
*   Basic knowledge of video conferencing concepts and terminology.

How This Guide is Organized

The following typographic conventions are used in this guide to distinguish types of in-text information.

Table 1-1   Typographic Conventions

Convention	Description
Bold	Highlights interface items such as menus, soft keys, flag names, and directories. Also used to represent menu selections and text entry to the phone.
Italics	Used to emphasize text, to show example values or inputs, file names and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Underlined Blue	Used for URL links to external Web pages or documents. If you click on text in this style, you will be linked to an external document or Web page.
Blue Text	Used for cross referenced page numbers in the same or other chapters or documents. If you click on blue text, you will be taken to the referenced section. Also used for cross references. If you click the italic cross reference text, you will be taken to the referenced section.
<variable name>	Indicates a variable for which you must enter information specific to your installation, endpoint, or network. For example, when you see <IP address>, enter the IP address of the described device.
>	Indicates that you need to select an item from a menu. For example, **Administration > System Information** indicates that you need to select **System Information** from the *Administration* menu.

About the Polycom® RMX 1800 System

The *Polycom RMX 1800* system is a high performance, scalable, IP-network (H.323 and SIP) MCU that provides feature-rich and easy-to-use multipoint voice and video conferencing.

The MCU can be used as a standalone device to run voice and video conferences or it can be used as part of a solution provided by Polycom. This solution may include the following components:

*   *Polycom® RSS™ 4000* - provides one-touch recording and secure playback on video conferencing systems, tablets and smartphones, or from your Web browser.
*   *Polycom® Distributed Media Application™* (DMA™) - provides call control and MCU virtualization with carrier-grade redundancy, resiliency and scalability.
*   *Polycom® RealPresence® Access Director™ (RPAD)* - removes communication barriers and enables internal and external teams to collaborate more easily and effectively over video.

The following diagram describes the multipoint video conferencing configuration with the Collaboration Server as a standalone system.
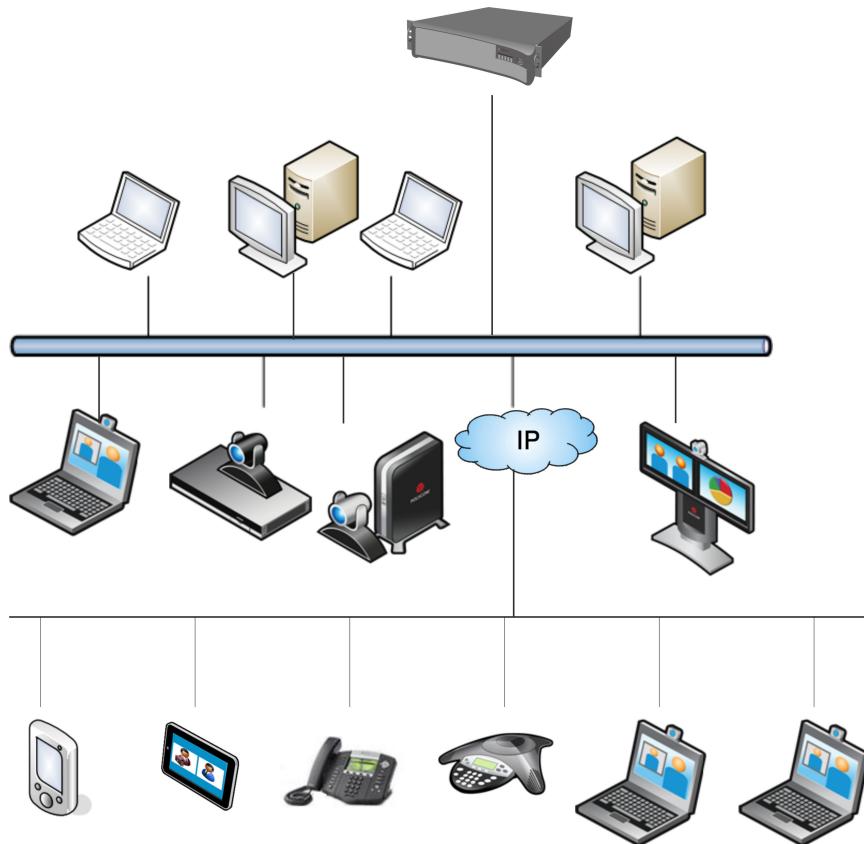
Figure 1-1 *Multipoint Video Conferencing using a Polycom Collaboration Server*

The Polycom RMX 1800 unit can be controlled via the LAN by the *Collaboration Server Web Client* application using Internet Explorer® installed on the user's workstation, or the RMX Manager application. The RMX Manager can control several Collaboration Server units. For more information about the RMX Manager see "*RMX Manager Application*" on page **18-1**.

Network Services Guidelines

IP Networks

In the Polycom® RMX 1800, system management and IP conferencing are performed on separate LAN ports. Management uses Lan1 and IP network Services use Lan2. When enabling multiple services, management and the IP network service (1) share Lan1, the second IP network service (2) uses Lan2. The networks can be separated in Maximum Security Environments.

Workstation Requirements

The *Collaboration Server Web Client* and *RMX Manager* applications can be installed in an environment that meets the following requirements:

- **Minimum Hardware** – Intel® Pentium® III, 1 GHz or higher, 1024 MB RAM, 500 MB free disk space.
- **Workstation Operating System** – Microsoft® Windows® XP, Vista®, Windows® 7.
- **Network Card** – 10/100 Mbps.
- **Web Browser** - Microsoft® Internet Explorer® Version 7, 8 and 9.
- Collaboration Server Web client and RMX Manager are optimized for display at a resolution of 1280 x 800 pixels and a magnification of 100%.

RMX 1800 users need to download .Net Framework 2.0 SP1 or above from the official Microsoft website and install the software. Internet Explorer must be enabled to allow running Signed ActiveX. If ActiveX installation is blocked please see *Polycom RealPresence Collaboration Server (RMX) 1800 Administrator's Guide*, "*ActiveX Bypass"* on page **19-52**.

Collaboration Server Web Client does not support larger Windows text or font sizes. It is recommended to set the text size to 100% (default) or Normal in the Display settings in Windows Control Panel on all workstations. Otherwise, some dialog boxes might not appear properly aligned. To change the text size, select **Control Panel>Display**. For Windows XP, click the **Appearance** tab, select **Normal** for the Font size and click **OK**. For Windows 7, click the **Smaller - 100%** option and click **OK**.

When installing the *Collaboration Server Web Client*, Windows Explorer **>Internet Options> Security Settings** must be set to *Medium* or less.

It is not recommended to run Collaboration Server Web Client and *Polycom CMAD* applications simultaneously on the same workstation.

For Windows 7™ Security Settings, see the *Polycom RMX 1800 Getting Started Guide*, "*Microsoft Windows 7™ Security Settings"* on page **1-10**.

For Internet Explorer 8 configuration, see the *Polycom RMX 1800 Getting Started Guide*, "*Microsoft Windows 7™ Security Settings"* on page **1-10**.

2

Conference Profiles

Profiles stored on the MCU enable you to define all types of conferences. Profiles include conference parameters such as Conference Line Rate, People and Content resolution and settings, Video Layout, Encryption, Lost Packet Recovery, etc.

The maximum number of *Conference Profiles* that can be defined is 40.

Conference Profiles are assigned to Conferences, Meeting Rooms, Reservations and Entry Queues. The same *Profile* can be assigned to different conferencing entities. When modifying the *Profile* parameters, the changes will be applied to all the conferencing entities to which the profile is assigned. Profile changes are not implemented in or affect ongoing conferences.

Conference Profile options differ according to the selected *Conference Type*. AVC (Advanced Video Codec) Conferencing Mode offers Continuous Presence (CP) conferences and a special functional conference - Operator Conferences.

Conferences based on *Profiles* can be saved to *Conference Templates* along with all participant parameters, including their *Personal Layout* and *Video Forcing* settings, enabling administrators and operators to create, save, schedule and activate identical conferences. For more information see Chapter 11, "*Conference Templates*" .

Conferencing Mode

The MCU system offers Transcoding - AVC Conferencing.

A transcoded CP (Continuous Presence) conference is also described as an AVC (Advanced Video Coding) conference. It supports the standard video protocols. In this mode, video is received from all the endpoints using different line rates, different protocols (SIP, H.323) and video parameters:

- Video protocols: H.261, H.263, H.264 Base and High profile
- Video Resolutions: from QCIF, CIF and up to 1080p
- Frame rates up to 60 fps

The MCU process the received video, transcodes it and send the resulting video streams to the endpoints. The video processing that is required differs according to the video session set for the conference, with all the processing performed by the MCU. For more details, see "*AVC Conferencing - Continuous Presence (CP) Conferencing*" on page **2-2**.

AVC Conferencing - Continuous Presence (CP) Conferencing

All endpoints have AVC capabilities and can connect to AVC conferences running on the MCU. AVC-based Endpoints can connect using different signaling protocols and different video protocols.

The dynamic Continuous Presence (CP) capability of the Collaboration Server system enables viewing flexibility by offering multiple viewing options and window layouts for video conferencing.

Endpoints can connect to the conference using any signaling protocol (H.323, SIP), line rate (up to a maximum line rate defined for the conference), Video Protocol (H.261, H.263, H.264 Base and High Profile) and at any resolution and frame rate (provided they meet the minimum requirements set for the conference).

In Continuous Presence conferences, the MCU receives the video stream from each endpoint at the video rate, video resolution and frame rate that it is capable of sending, and it superimposes all the received streams into one video stream that includes the input from the other endpoints arranges in the selected video layout.

Participants do not see themselves in the video layout. By Default, the speaker is shown in the top left layout cell in symmetric layouts, in the larger cell in asymmetric layouts, or in full screen. The speaker sees the previous speakers (their number depends on the number of cells on the speaker's layout.

The Continuous Presence video session offers layouts to accommodate different numbers of participants and conference settings including support of the VUI annex to the H.264 protocol for endpoints that transmit wide video instead of 4CIF resolution. Each participant can select his/her layout for viewing during the conference, as can be seen in Figure 2-1.

For conferences with more participants than display squares, the Collaboration Server dynamic video mix capability allows the viewed sites to be modified throughout the conference. The displayed layout can be changed during an ongoing conference, allowing a participant to view different screen layouts of the other conference participants. These layout options allow conferences to have greater flexibility when displaying a large number of participants and maximizes the screen's effectiveness.
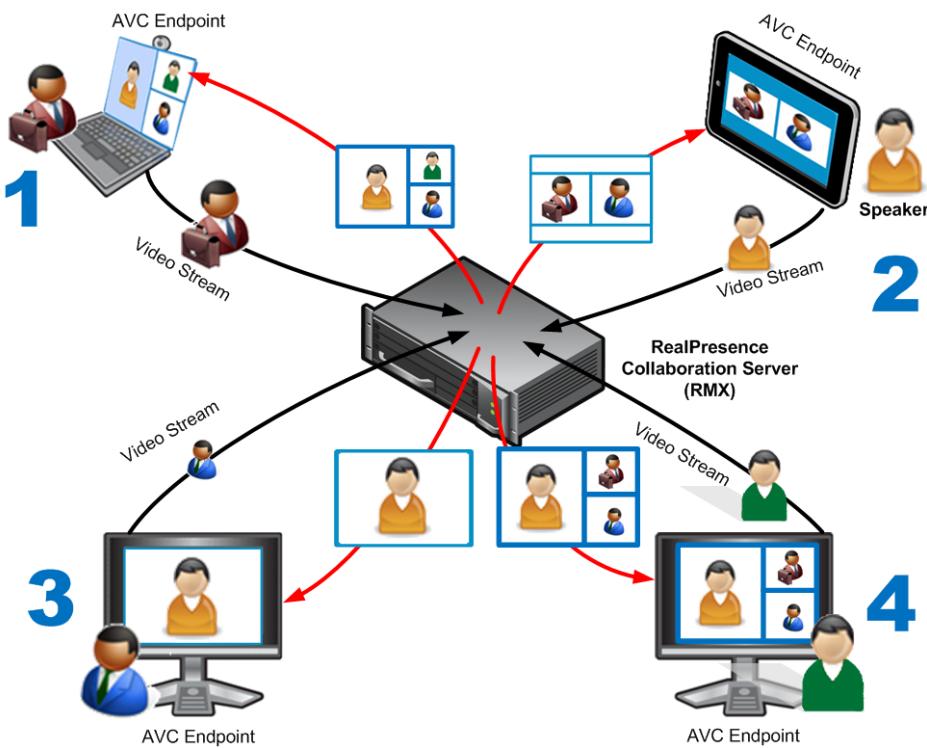
Figure 2-1 AVC Continuous Presence (CP) video streams and built layouts

Video quality in Continuous Presence conferences is affected by the conference line rate (that determines the maximum line rate to be used by the connecting endpoints), and the video capabilities of the endpoints such as the video protocol, video resolution and frame rate. Content sharing is available in all CP conferences.

This requires extensive processing of the video sent to each participant in the conference. The higher the video rate and resolution, the more processing power is required.

By default every conference, Entry Queue and Meeting Room has the ability to declare the maximum CP resolution as defined for the system. This includes conferences launched by the *Collaboration Server Web Client* and conferences started via the API.

CP conferencing is defined in the Conference profile by settings the following main features:
- Setting the *Conferencing Mode* to **AVC only**
- Conference Line Rate
- Video Quality – Motion or Sharpness
- Video Layout

Video Protocol Support in CP Conferences

The video protocol selected by the system determines the video compression standard used by the endpoints. In Continuous Presence conferences, the system selects the best video protocol for each of the endpoint according to the endpoint's capabilities.

The following Video protocols are supported in CP conferences:
- **H.261 -** the legacy video compression algorithm mandatory to all endpoints. It is used by endpoints that do not support other protocols.

- **H.263 -** a video compression algorithm that provides a better video quality than H.261. This standard is not supported by all endpoints.
- **H.264** Base Profile **-** a video compression standard that offers improved video quality, especially at line rates lower than 384 Kbps.

  H.264 High Profile allows higher quality video to be transmitted at lower line rates.

AVC Conferencing Parameters

Basic Conferencing Parameters

When defining a new video Profile, you select the parameters that determine the video display on the participant's endpoint and the quality of the video. When defining a new conference Profile, the system uses default values for Continuous Presence (CP) standard conferencing. Continuous Presence conferencing enables several participants to be viewed simultaneously and each connected endpoint uses its highest video, audio and data capabilities up to the maximum line rate set for the conference.

The main parameters that define the quality of a video conference are:

- **Line (Bit) Rate -** The transfer rate of video and audio streams. The higher the line (bit) rate, the better the video quality.
- **Audio Algorithm -** The audio compression algorithm determines the quality of the conference audio.
- **Video protocol, video format, frame rate, annexes, and interlaced video mode** - These parameters define the quality of the video images. The Collaboration Server will send video at the best possible resolution supported by endpoints regardless of the resolution received from the endpoints.
  — When *Sharpness* is selected as the *Video Quality* setting in the *Conference Profile*, the Collaboration Server will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps.
  — *H.264 High Profile* protocol provides better compression of video images in line rates lower than 384 Kbps and it will be automatically selected for the endpoint if it supports H.264 *High Profile*. If the endpoint does not support H.264 High Profile, the Collaboration Server will try H.264 Base Profile which provides good compression of video images in line rates lower than 384 Kbps (better than H.263 and not as good as H.264 *High Profile)*.
  — When working with Collaboration Servers at low bit rates (128, 256, or 384Kbps), HDX endpoints will transmit SD15 resolution instead of 2CIF resolution.

  When using a full screen (1x1) conference layout, the Collaboration Server transmits the same resolution it receives from the endpoint.
- **Lost Packet Recovery (LPR) -** LPR creates additional packets that contain recovery information used to reconstruct packets that are lost during transmission.
- Supported resolutions:
  — **H.261 CIF/QCIF –** Is supported in Continuous Presence (CP) conferences at resolutions of 288 x 352 pixels (CIF) and 144 x 176 pixels (QCIF). Both resolutions are supported at frame rates of up to 30 frames per second.
  — **H.263 4CIF** - A high video resolution available to H.263 endpoints that do not support H.264. It is only supported for conferences in which the video quality is set to sharpness and for lines rates of 384kbps to 1920kbps.
  — **Standard Definition (SD)** - A high quality video protocol which uses the H.264 and H.264 High Profile video algorithms. It enables compliant endpoints to

connect to Continuous Presence conferences at resolutions of 720X576 pixels for PAL systems and 720X480 pixels for NTSC systems. For more information, see "*Video Resolutions in AVC-based CP Conferencing*" on page **3-1**.

— **High Definition (HD)** – HD is an ultra-high quality video resolution that uses he H.264 and H.264 High Profile video algorithms. Endpoints are able to connect to conferences at the following resolutions:

- **720p** (1280 x 720 pixels)
- **1080p** (1920 x 1080 pixels)

For more information, see "*Video Resolutions in AVC-based CP Conferencing*" on page **3-1**.

Supplemental Conferencing Features

In addition to *Standard Conferencing* the following features can be enabled:

- **H.239 –** Allows compliant endpoints to transmit and receive two simultaneous streams of conference data to enable Content sharing. H.239 is also supported in cascading conferences. Both H.263 and H.264 Content sharing protocols are supported. If all endpoints connected to the conference have H.264 capability, Content is shared using H.264, otherwise Content is shared using H.263.
  For more information, see **"***Content Sharing***" on page 4-1.**

- **Lecture Mode –** The lecturer is seen by all participants in full screen while the lecturer views all conference participants in the selected video layout.
  For more information, see **"***Lecture Mode***" on page 4-38.**

- **Presentation Mode (CP Conferences only) –** When the current speaker's speech exceeds a predefined time (30 seconds), the conference layout automatically changes to full screen, displaying the current speaker as the conference lecturer on all the participants' endpoints. During this time the speaker's endpoint displays the previous conference layout. When another participant starts talking, the Presentation Mode is cancelled and the conference returns to its predefined video layout. Presentation mode is available with *Auto Layout* and *Same Layout*.

  — If the speaker in a video conference is an Audio Only participant, the Presentation Mode is disabled for that participant.

  — Video forcing works in the same way as in Lecture Mode when Presentation Mode is activated, that is, forcing is only enabled at the conference level, and it only applies to the video layout viewed by the lecturer.

- **Encryption –** Used to enhance media security at conference and participant levels. For more information, see "*Media Encryption*" on page **4-27**.

- **Conference Recording -** The Collaboration Server enables audio and video recording of conferences using Polycom RSS recording system.

Operator Conferences (CP only Conferences)

Offers additional conference management capabilities to the Collaboration Server users, enabling them to attend to participants with special requirements and acquire participant details for billing and statistics. This service is designed usually for large conferences that require the personal touch. For more information, see Chapter 10, "*Operator Assistance & Participant Move*" on page **10-1**

Default Profile Settings in CP Conferencing Mode

The Collaboration Server is shipped with a default *Conference Profile* for CP conferences which allows users to immediately start standard ongoing CP conferences. These are also the default settings when creating a new Profile. The default settings are as follows:

Table 2-1   Default CP Only Conference Profile Settings

Setting	Value
Profile Name	Factory_Video_Profile
Line Rate	384Kbps
Operator Conference	Disabled
Encryption	Disabled
Packet Loss Compensation (LPR and DBA)	Disabled
Auto Terminate	• After last participant quits - Enabled • When last participant remains - Disabled
Auto Redialing	Disabled
Exclusive Content Mode	Disabled
Enable FECC	Enabled
Video Quality	Sharpness
Maximum Resolution	Auto
Content Settings	Graphics
Content Protocol	H.263 & H.264 HD Auto Selection
Presentation Mode	Enabled
Same Layout	Disabled
Lecturer View Switching	Disabled
Auto Scan Interval	Disabled (10)
Auto Layout	Enabled
Mute participants except the lecturer	Disabled
Speaker change threshold	Auto
Skin	Polycom
IVR Name	Conference IVR Service
Recording	Disabled
Site Names display	Disabled
Network Services - SIP Registration	Disabled

Table 2-1   *Default CP Only Conference Profile Settings (Continued)*

Setting	Value
Network Services - Accept Calls	Enabled

This *Profile* is automatically assigned to the following conferencing entities:

Name	ID
Meeting Rooms	
Maple_Room	*1001*
Oak_Room	*1002*
Juniper_Room	*1003*
Fig_Room	*1004*
Entry Queue	
Default EQ	*1000*

Viewing Profiles

Conference Profiles are listed in the *Conference Profiles* list pane.

To list Conference Profiles:

1 In the *Collaboration Server Management* pane, expand the *Rarely Used* list.

2 Click the **Conference Profiles** button.

The *Conference Profiles* are displayed in the *List* pane.

The number of the currently defined Conference Profiles appears in the title of the list pane.

The following *Conference Profile* properties are displayed in the *List* pane:

Table 2-2   Conference Profiles Pane Columns

Field	Description
Name	The name of the *Conference Profile*.
Layout	Displays either "*Auto Layout*" or an icon of the layout selected for the profile. For information about video layouts, see Table 2-9 "*Video Layout Options"* on page **2-19**.
Line Rate	The maximum bit rate in kbps at which endpoints can connect to the conference.
Routing Name	Displays the Routing Name defined by the user or automatically generated by the system.
Encryption	Displays if media encryption is enabled for the Profile. For more information see "*Media Encryption"* on page **4-27**.

Profile Toolbar

The Profile toolbar provides quick access to the Profile functions:

Table 2-3   Profile Tool bar buttons

Button	Button Name	Description
	New Profile	To create a new Profile.
	Delete Profile	To delete a Profile, click the Profile name and then click this button.
	Import Profile	To import Conference Profiles from another MCU in your environment.
	Export Profile	To export Conference Profiles to a single XML file that can be used to import the Conference Profiles on multiple MCUs.

Modifying an Existing Profile

You can modify any of the Profile's parameters but you cannot rename the *Profile*.

To modify the Profile Properties:

1 In the *Conference Profiles* list, double -click the *Profile* icon or right-click the *Profile* icon, and then click **Profile Properties**.

The Profile *Properties - General* dialog box opens.

Deleting a Conference Profile

To delete a Conference Profile:

1 In the *Conference Profiles* list, select the *Conference Profile* you want to delete.

2 Click the **Delete Profile** (✖) button.
or
Right-click the *Conference Profile* to be deleted and select
Delete Profile from the drop-down menu.

A confirmation dialog box is displayed.

3 Click **OK** in the confirmation dialog box.

4 The *Conference Profile* is deleted.

> A *Conference Profile* cannot be deleted if it is being used by Meeting Rooms, Entry Queues, SIP Factories and Reservations.
> A Profile that is assigned to only one ongoing conference and no other conferencing entity can be deleted.

Defining New Profiles

Profiles are the basis for the definition of all ongoing conferences, *Reservations*, *Meeting Rooms*, *Entry Queues*, and *Conference Templates* and they contain only conference properties.

Defining AVC - CP Conferencing Profiles

To define a new Profile:

1   In the *RMX Management* pane, click **Conference Profiles**.

2   In the *Conference Profiles* pane, click the **New Profile** button.
The *New Profile – General* dialog box opens.
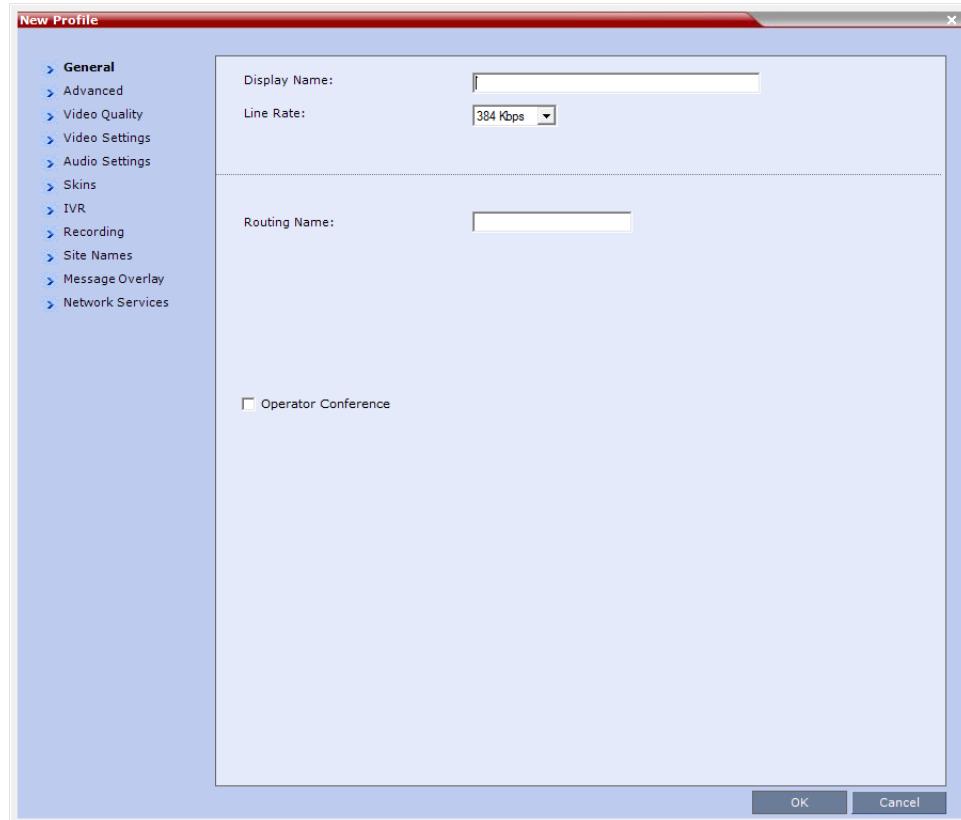
3   Define the *Profile* name and, if required, the *Profile - General* parameters:

Table 2-4   *New AVC-CP Profile - General Parameters*

Field/Option	Description
Display Name	Enter a unique Profile name, as follows: • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. It is recommended to use a name that indicates the Profile type, such as Operator conference or Video Switching conference. **Note:** This is the only parameter that must be defined when creating a new profile. **Note:** This field is displayed in all tabs.

Table 2-4 *New AVC-CP Profile - General Parameters (Continued)*

Field/Option	Description
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate. The default setting is 384 Kbps. **Notes:** • This field is displayed in all tabs.
Routing Name	Enter the *Profile* name using ASCII characters set. The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows: • If an all ASCII text is entered in Display Name, it is used also as the Routing Name. • If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.
Operator Conference	Select this option to define the profile of an Operator conference. For more information, see Chapter 10, "*Operator Assistance & Participant Move*" on page **10-1**.

4 Click the **Advanced** tab.

The *New Profile – Advanced* dialog box opens.
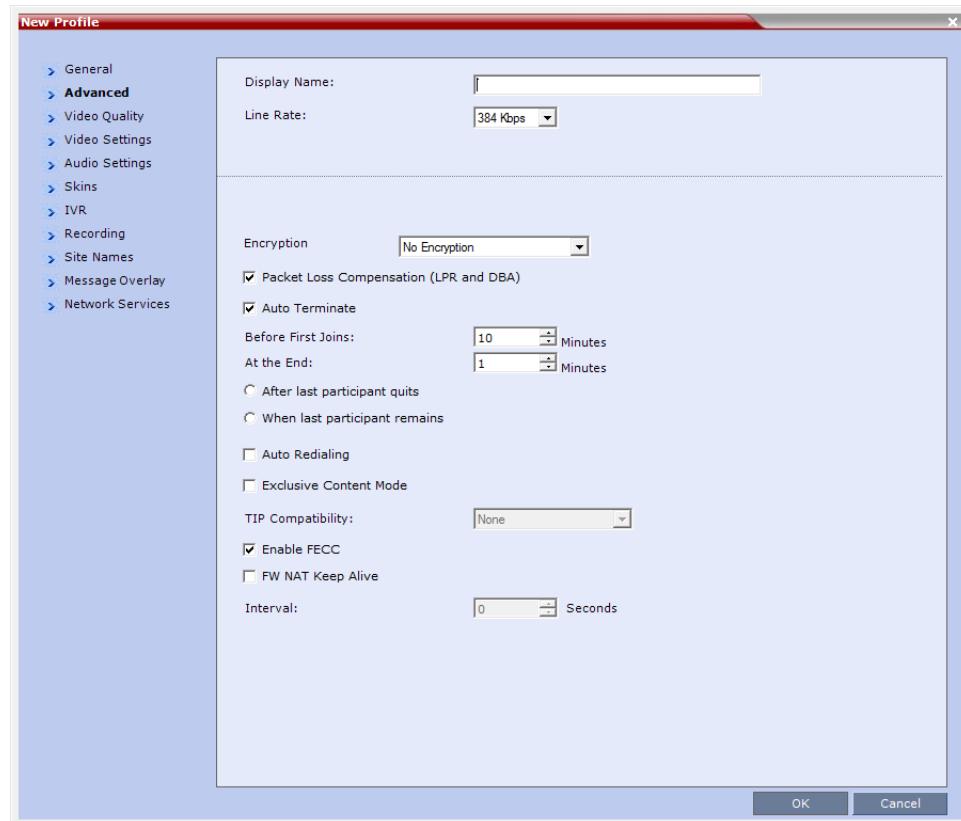
5   Define the following parameters:

Table 2-5   *New AVC-CP Profile - Advanced Parameters*

Field/Option	Description
Encryption	Select the Encryption option for the conference: • **Encrypt All** - Encryption is enabled for the conference and all conference participants must be encrypted. • **No Encryption** - Encryption is disabled for the conference. • **Encrypt when Possible** - enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. For connection guidelines see "*Mixing Encrypted and Non-encrypted Endpoints in one Conference"* on page **4-28**. For more information, see "*Media Encryption"* on page **4-27**.
LPR	When selected, *Lost Packet Recovery* creates additional packets that contain recovery information used to reconstruct packets that are lost during transmission. For more information, see "*Packet Loss Compensation (LPR and DBA)"* on page **4-35**.
Auto Terminate	When selected (default), the conference automatically ends when the termination conditions are met: ***Before First Joins*** — No participant has connected to a conference during the *n* minutes after it started. Default idle time is 10 minutes. ***At the End - After Last Quits*** — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute. ***At the End - When Last Participant Remains*** — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). **Note:** The selection of this option is automatically cleared and disabled when the *Operator Conference* option is selected. The Operator conference cannot automatically end unless it is terminated by the Collaboration Server User.
Auto Redialing	The *Auto Redialing* option instructs the Collaboration Server to automatically redial *H.323* and *SIP* participants that have been abnormally disconnected from the conference. • *Auto Redialing* is disabled by default. • *Auto Redialing* can be enabled or disabled during an ongoing conference using the *Conference Properties – Advanced* dialog box. • The Collaboration Server will not redial an endpoint that has been disconnected from the conference by the participant. • The Collaboration Server will not redial an endpoint that has been disconnected or deleted from the conference by an operator or administrator.

Table 2-5   *New AVC-CP Profile - Advanced Parameters (Continued)*

Field/Option	Description
Exclusive Content Mode	Select the *Exclusive Content Mode* check box to limit the Content broadcasting to one participant, preventing other participants from interrupting the Content broadcasting while it is active. For more details, see "*Exclusive Content Mode"* on page **4-16**.
Enable FECC	This option is enabled by default, allowing participants in the conference to control the zoom and PAN of other endpoints in the conference via the FECC channel. Clear this check box to disable this option for all conference participants.
FW NAT Keep Alive	The MCU can be configured to send a *FW NAT Keep Alive* message at specific Intervals for the *RTP*, *UDP* and *BFCP* channels. For more information see "*FW (Firewall) NAT Keep Alive"* on page **16-25**.
Interval	If needed, modify the *NAT Keep Alive Interval* field within the range of 1 - 86400 seconds.For more information see "*FW (Firewall) NAT Keep Alive"* on page **16-25**.

6   Click the **Video Quality** tab.

The *New Profile – Video Quality* dialog box opens.
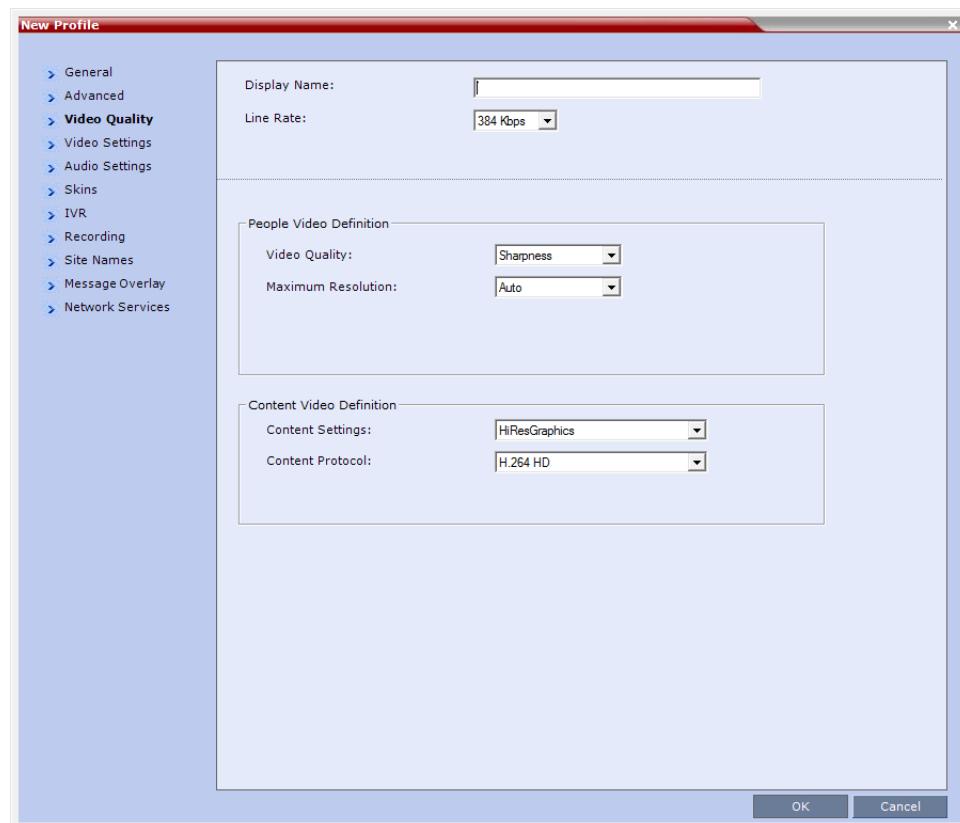
7 Define the following parameters:

Table 2-6   New AVC Profile - Video Quality Parameters

Field/Option	Description
People Video Definition	
Video Quality	Sharpness is the only supported content format that supports higher video resolutions. Depending on the amount of movement contained in the conference video, select either: • **Motion** – for a higher frame rate without increased resolution. When selected, *Video Clarity* is disabled. • **Sharpness** – for higher video resolution and requires more system resources. **Note:** When Sharpness is selected as the *Video Quality* setting in the conference Profile, the Collaboration Server will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps. For more information, see "*Video Resolutions in AVC-based CP Conferencing*" on page **3-1**.
Maximum Resolution	This setting overrides the *Maximum Resolution* setting of the *Resolution Configuration* dialog box. The administrator can select one of the following *Maximum Resolution* options: • *Auto* (default) - The *Maximum Resolution* remains as selected in the *Resolution Configuration* dialog box. • *CIF* • *SD* • *HD720* • *HD1080* *Maximum Resolution* settings can be monitored in the *Profile Properties - Video Quality* and *Participant Properties - Advanced* dialog boxes. **Notes:** • The *Resolution* field in the *New Participant - Advanced* dialog box allows *Maximum Resolution* to be **further limited** per participant endpoint. • The *Maximum Resolution* settings for conferences and participants cannot be changed during an ongoing conference.

Table 2-6   *New AVC Profile - Video Quality Parameters (Continued)*

Field/Option	Description
Content Video Definition	
Content Settings	Select the transmission mode for the Content channel: • ***Graphics*** — basic mode, intended for normal graphics • ***Hi-res Graphics*** — a higher bit rate intended for high resolution graphic display • ***Live Video*** — Content channel displays live video • ***Customized Content Rate*** — manual definition of the Conference Content Rate**,** mainly for cascading conferences. Selection of a higher bit rate for the *Content* results in a lower bit rate for the people channel. For a detailed description of each of these options, see "*Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode"* on page **4-5**.

Content Protocol	• **H.263**
	   • *Content* is shared using the *H.263* protocol.
	   • Use this option when most of the endpoints support *H.263* and some endpoints support *H.264*.
	• **H.263 & H.264 Auto Selection**
	   • *Content* is shared using *H.263* if a mix of H.263-supporting and *H.264*-supporting endpoints are connected.
	   • *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
	• **H.264 Cascade**
	   • All *Content* is shared using the *H.264* content protocol and is optimized for use in *Cascaded Conferences*.
	• **H.264 HD** (Default)
	   • Ensures high quality *Content* when most endpoints support *H.264* and *HD Resolutions*.
	For more information, see "*Content Protocols"* on page **4-7** and "*Defining Content Sharing Parameters for a Conference"* on page **4-3**.

8   Click the **Video Settings** tab.
The *New Profile - Video Settings* dialog box opens.
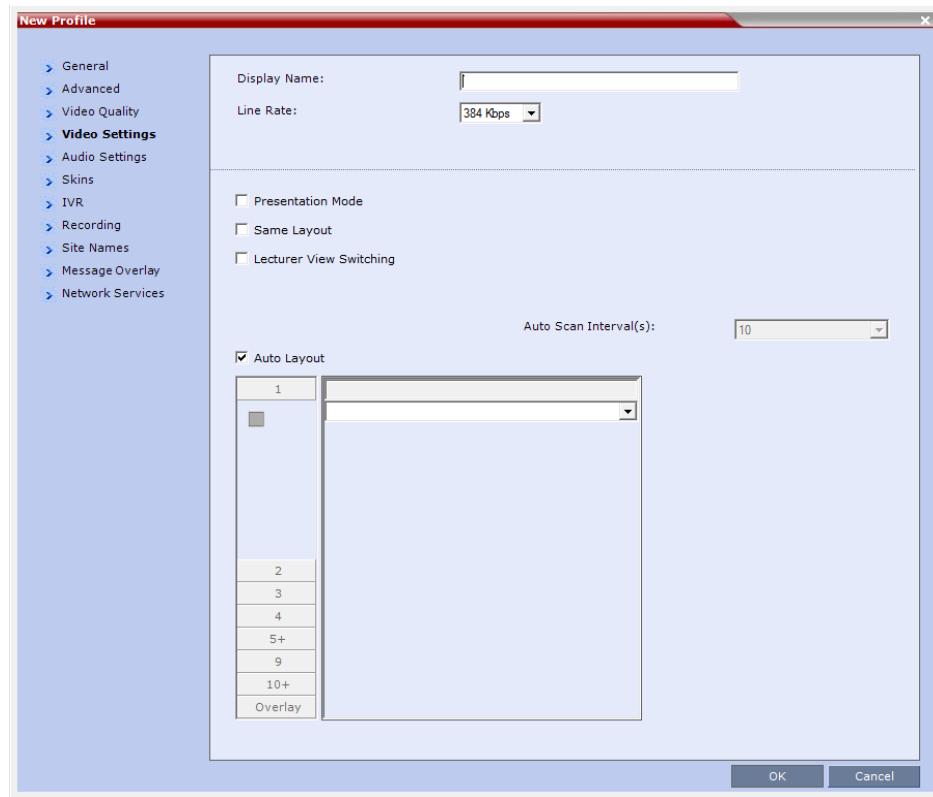
9   Define the video display mode and layout using the following parameters:

Table 2-7   New AVC CP Profile - Video Settings Parameters

Field/Option	Description
Presentation Mode	Select this option to activate the Presentation Mode. In this mode, when the current speaker speaks for a predefined time (30 seconds), the conference changes to Lecture Mode. When another participant starts talking, the Presentation Mode is cancelled and the conference returns to the previous video layout.
Same Layout	Select this option to force the selected layout on all participants in a conference. Displays the same video stream to all participants and personal selection of the video layout is disabled. In addition, if participants are forced to a video layout window, they can see themselves.
Lecture View Switching	Select this option to enable automatic switching of participants on the Lecturer's screen when Lecture Mode is enabled for the conference. The automatic switching is enabled when the number of participants exceeds the number of video windows displayed on the Lecturer's screen. **Note:** Lecture Mode is enabled in the *Conference Properties – Participants* tab. For more information, see "*Lecture Mode*" on page **4-38**.

Table 2-7 *New AVC CP Profile - Video Settings Parameters (Continued)*

Field/Option	Description
Auto Scan Interval(s)	Select the time interval, 5 - 300 seconds, that *Auto Scan* uses to cycle the display of participants that are not in the conference layout in the selected cell. *Auto Scan* is often used in conjunction with *Customized Polling* which allows the cyclic display to be set to a predefined order for a predefined time period.
Auto Layout	When selected (default), the system automatically selects the conference layout based on the number of participants currently connected to the conference. When a new video participant connects or disconnects, the conference layout automatically changes to reflect the new number of video participants. For more information, see Table 2-8 "*Auto Layout – Default Layouts in CP Conferences"* on page **2-17**. Clear this selection to manually select a layout for the conference. The default Auto Layout settings can be customized by modifying default Auto Layout system flags in the System Configuration file. For more information see, "*Auto Layout Configuration"* on page **20-21**. **Note:** In some cases, the default layout automatically selected for the conference contains more cells than the number of connected participants, resulting in an empty cell. For example, if the number of connected participants is 4, the default layout is 2x2, but as only 3 participants are displayed in the layout (the participants do not see themselves), one cell is empty.

Table 2-8 *Auto Layout – Default Layouts in CP Conferences*

Number of Video Participants	Auto Layout Default Settings
0–2	
3	
4–5	
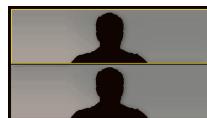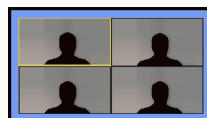
Table 2-8 *Auto Layout – Default Layouts in CP Conferences (Continued)*

Number of Video Participants	Auto Layout Default Settings
6–7	
8-10	
11	
12+	
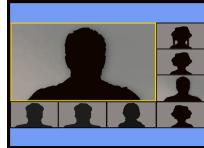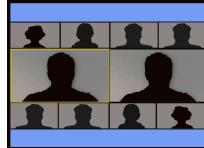
In layout 2+8, the two central windows display the last two speakers in the conference: the current speaker and the "previous" speaker. To minimize the changes in the layout, when a new speaker is identified the "previous" speaker is replaced by the new speaker while the current speaker remains in his/her window.

The Collaboration Server supports the VUI addition to the H.264 protocol for endpoints that transmit wide video (16:9) in standard 4SIF resolution.

10 To select the *Video Layout* for the conference, click the required number of windows from the layouts bar and then select the windows array. The selected layout is displayed in the *Video Layout* pane.

Table 2-9   *Video Layout Options*

Number of Video Windows	Available Video Layouts				
1					
2					
3					
4					
5+					
9					
10+					

11 Click the **Audio Settings** tab.
The *New Profile - Audio Settings* dialog box opens.
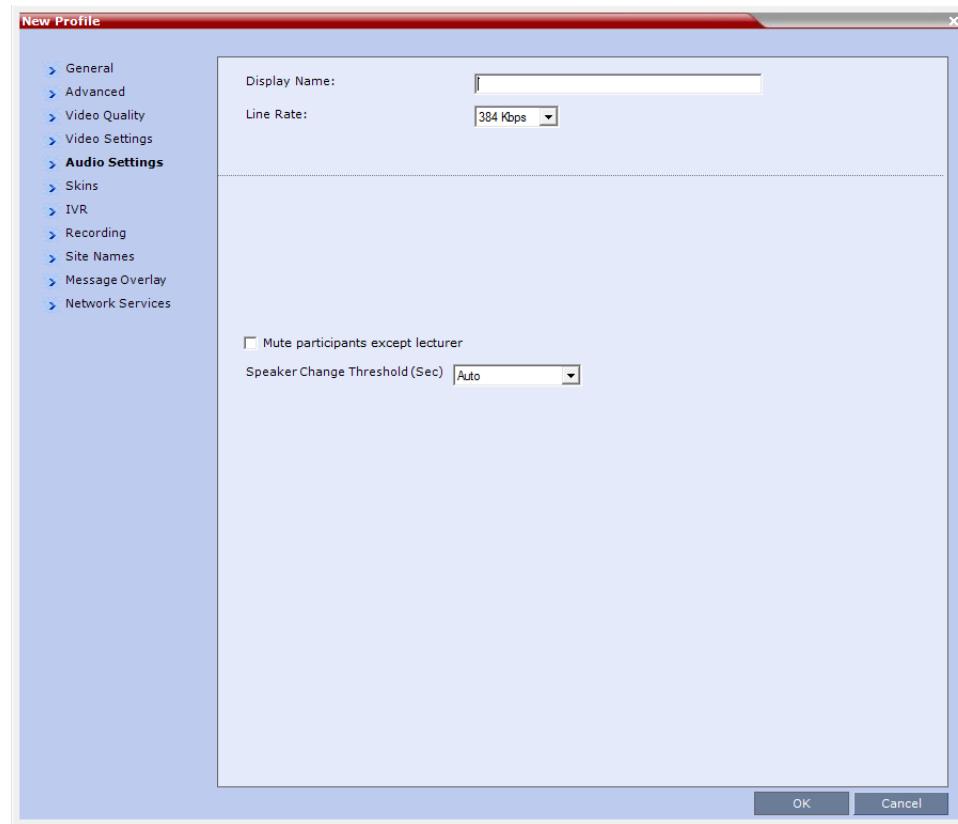
12 Define the following parameters:

Table 2-10 *New AVC Profile - Audio Settings Parameters*

Field/Option	Description
Mute participant except lecturer	When the *Mute Participants Except Lecturer* option is enabled, the audio of all participants in the conference except for the lecturer can be automatically muted upon connection to the conference. This prevents other conference participants from accidentally interrupting the lecture, or from a noisy participant affecting the audio quality of the entire conference. Muted participants cannot unmute themselves unless they are unmuted from the Collaboration Server Web Client/ RMX Manager. You can enable or disable this option during the ongoing conference. **Notes:** • When enabled, the mute indicator on the participant endpoints are not visible because the mute participants was initiated by the MCU. Therefore, it is recommended to inform the participants that their audio is muted by using the Closed Caption or Message Overlay functions. In the Collaboration Server Web Client/RMX Manager the mute by MCU indicator is listed for each muted participant in the *Audio* column in the *Participants* pane. • The *Mute Participants Except Lecturer* option can be disabled during an ongoing conference, thereby unmuting all the participants in the conference. • If the endpoint of the designated lecturer is muted when the lecturer connects to the conference, the lecturer remains muted until the endpoint has been unmuted. • When you replace a lecturer, the MCU automatically mutes the previous lecturer and unmutes the new lecturer. • When you disconnect a lecturer from the conference or the lecturer leaves the conference, all participants remain muted but are able to view participants in regular video layout until the you disable the *Mute Participants Except Lecturer* option. • A participant can override the *Mute Participants Except Lecturer* option by activating the *Mute All Except Me option* using the appropriate DTMF code, provided the participant has authorization for this operation in the *IVR Services*. The lecturer audio is muted and the participant audio is unmuted. You can reactivate the *Mute Participants Except Lecturer* option after a participant has previously activated the Mute All Except Me option. The participant is muted and the lecturer, if designated, is unmuted. • In cascaded conferences, all participants (including the link participants) are muted. Only the lecturer is not muted.

Table 2-10 *New AVC Profile - Audio Settings Parameters (Continued)*

Field/Option	Description
Speaker Change Threshold	The Speaker Change Threshold is the amount of time a participant must speak continuously before becoming the speaker. When defining or editing a conference profile, you can define the Speaker Change Threshold. Select the desired threshold: • Auto (Default, 3 seconds) • 1.5 seconds • 3 seconds • 5 seconds

13 Click the **Skins** tab to modify the background and frames.
The *New Profile - Skins* dialog box opens.
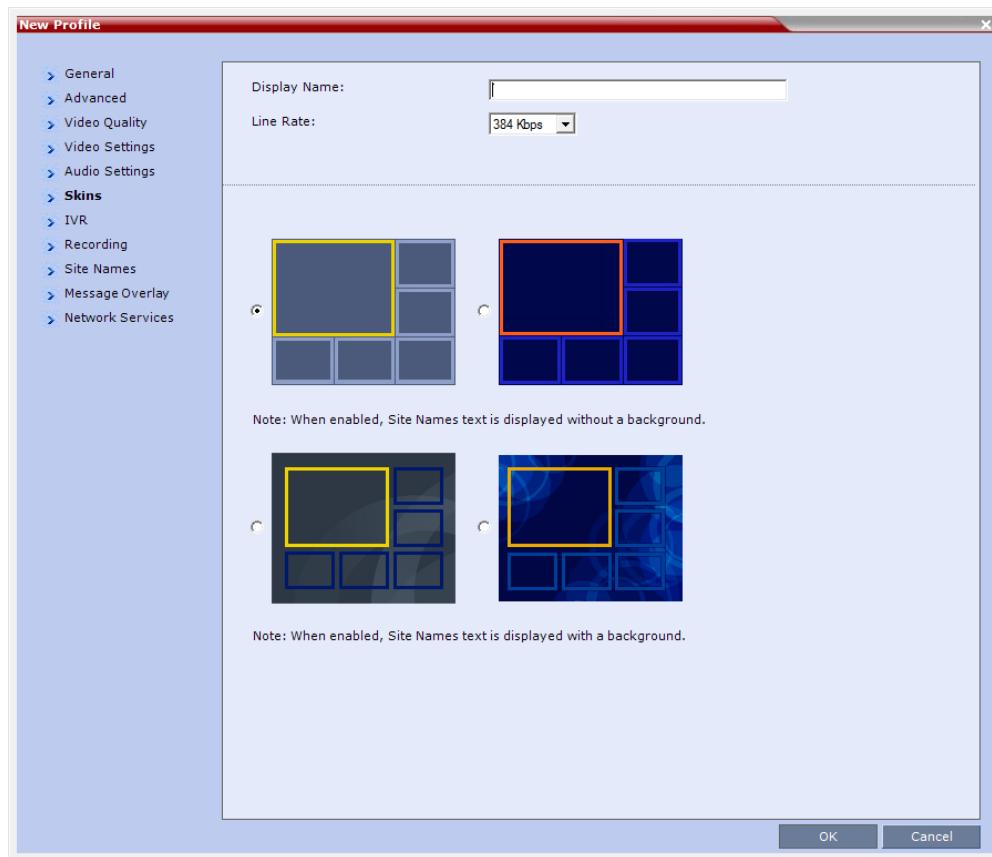
14 Select one of the *Skin* options.

15 Click **IVR** tab.

The *New Profile - IVR* dialog box opens.
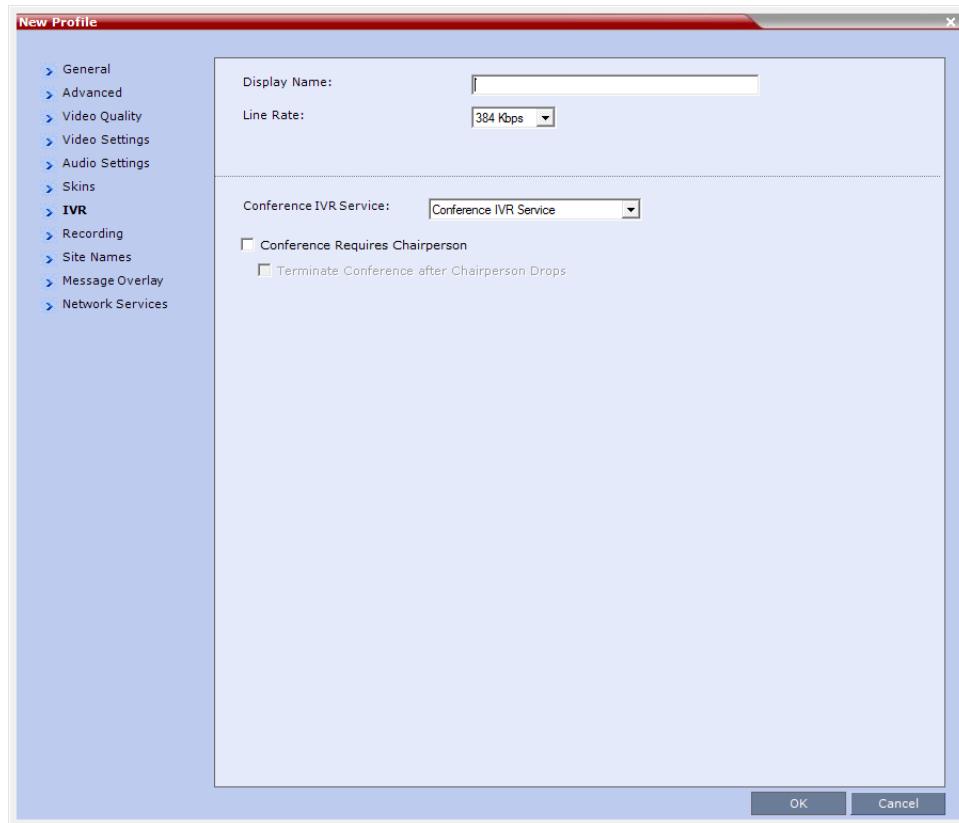
16 If required, set the following parameters:

Table 2-11 *New AVC CP Profile - IVR Parameters*

Field/Option	Description
Conference IVR Service	The default conference IVR Service is selected. You can select another conference IVR Service if required.
Conference Requires Chairperson	Select this option to allow the conference to start only when the chairperson connects to the conference and to automatically terminate the conference when the chairperson exits. Participants who connect to the conference before the chairperson are placed on *Hold* and hear background music (and see the *Welcome* video slide). Once the conference is activated, the participants are automatically connected to the conference. When the check box is cleared, the conference starts when the first participant connects to it and ends at the predefined time or according to the *Auto Terminate* rules when enabled.

Table 2-11 *New AVC CP Profile - IVR Parameters (Continued)*

Field/Option	Description
Terminate Conference after chairperson drops	When enabled, it allows a conference to be automatically terminated after the chairperson leaves. When the chairperson leaves, the *Chairperson Has Left* IVR message is played to all participants and the conference terminates. **Note:** If there is a single chairperson in the conference who is changed to a regular participant, the conference will be terminated as if the chairperson left. It is therefore recommended that before changing a single chairperson to regular participant, another participant first be changed to chairperson.

17 **Optional**. Click the **Recording** tab to enable conference recording with *Polycom RSS 4000*.

The *New Profile - Recording* tab opens.
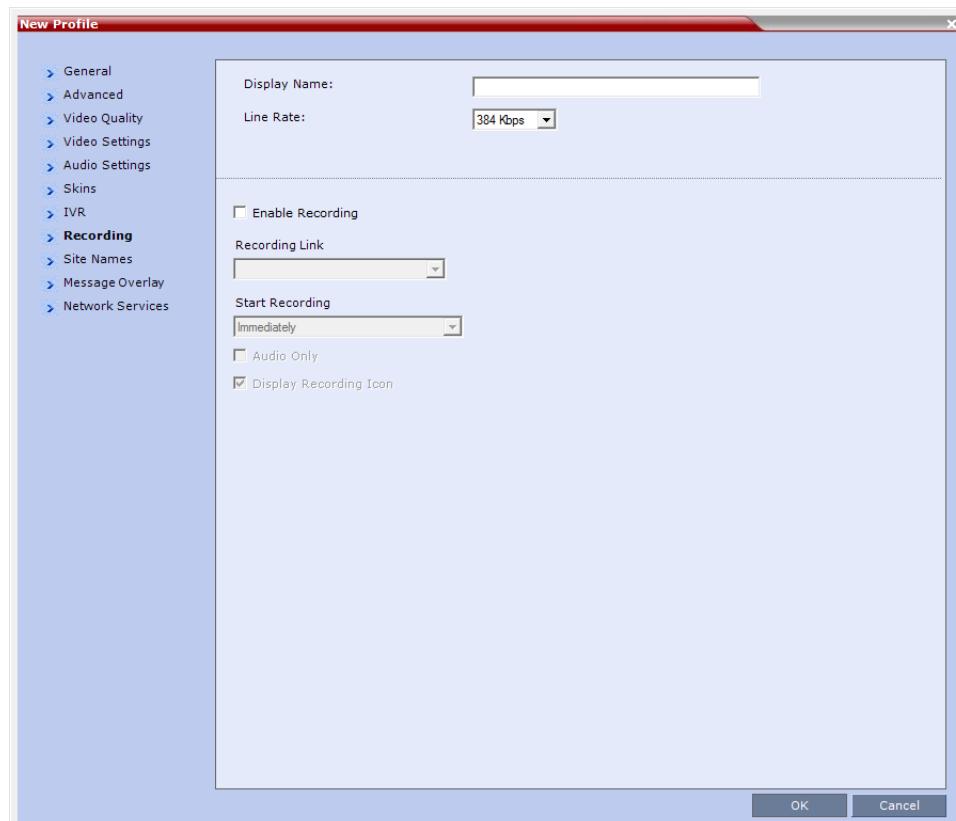
18 Define the following parameters:

Table 2-12 *New AVC Profile - Recording Parameters*

Parameter	Description
Enable Recording	Select this check box to enable the *Recording* settings. If no *Recording Links* are found an error message is displayed.

Table 2-12 New AVC Profile - Recording Parameters (Continued)

Parameter	Description
Recording Link	*Select the Recording Link to be used for conference recording. Recording Links defined on the Collaboration Server can be given a descriptive name and can be associated with a Virtual Recording Room (VRR) saved on the Polycom® RSS™ 4000 Version 8.5 Recording and Streaming Server (RSS). For more information see "Recording Conferences" on page* **13-1**.
Start Recording	Select one of the following: • **Immediately** – conference recording is automatically started upon connection of the first participant. • **Upon Request** – the operator or chairperson must initiate the recording (manual).
Audio Only	Select this option to record only the audio channel of the conference. **Note:** This option can be used only if there are Voice ports configured in the Video/Voice Port Configuration. For more information, see "*Forcing Video Resource Allocation to CIF Resolution" on page* **19-6**.
Display Recording Icon	This option is automatically selected to display a *Recording Indication* to all conference participants informing them that the conference is being recorded.
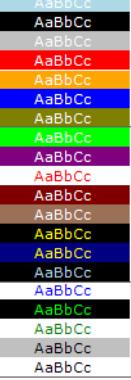
19 Click the **Site Names** tab to display the *Site Names* dialog box.
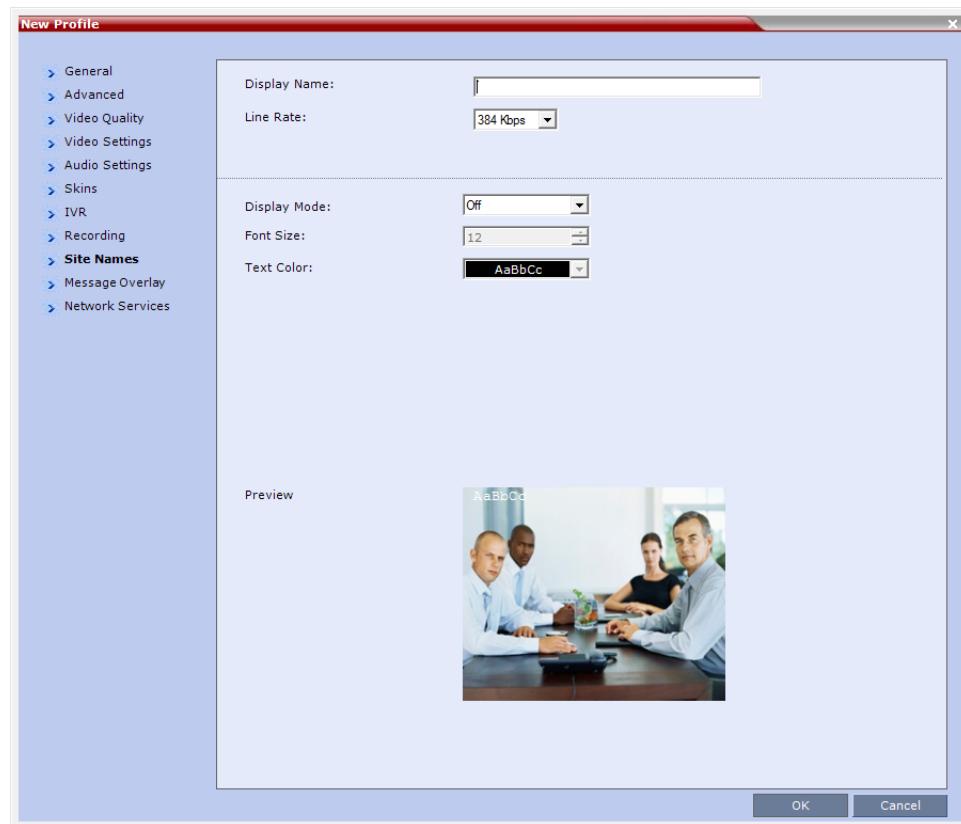
Using the *Site Name* dialog box, you can control the display of the site names by defining the font, size, color, background color and transparency and position within the Video Window. For a detailed description of the site names options see "*Site Names Definition*" on page **2-35**.

20 Define the following parameters:

Table 2-13 *New AVC-CP Profile - Site Names Parameters*

Field	Description
Display Mode	Select the display mode for the site names: • **Auto** - Display the *Site Names* for 10 seconds whenever the *Video Layout* changes. • **On** - Display the *Site Names* for the duration of the conference. • **Off** (default) - Do not display the *Site Names*. **Note:** If *Display Mode* is **Off**, all other fields in this tab are grayed and disabled.
Font Size	Click the arrows to adjust the font size (in points) for the *Site Names* display. **Range:** 9 - 32 points **Default:** 12 **Note:** Choose a *Font Size* that is suitable for viewing at the conference's video resolution. For example, if the resolution is *CIF*, a larger *Font Size* should be selected for easier viewing.
Background Color	Select the color of the *Site Names* display text. The color and background for *Site Names* display text is dependent on whether a *Plain Skin* or a *Picture Skin* was selected for the conference in the *Profile - Skins* tab. The choices are: **Plain Skin** **Picture Skin** **Default:** White Text No Background (For contrast, no background is shown as black when the text is white.) **Default:** White Text Red Background **Note:** Choose a *Background Color* combination that is suitable for viewing at the conference's video resolution. At low resolutions, it is recommended to select brighter colors as dark colors may not provide for optimal viewing.

21 Click the **Message Overlay** tab to display the *Message Overlay* dialog box.
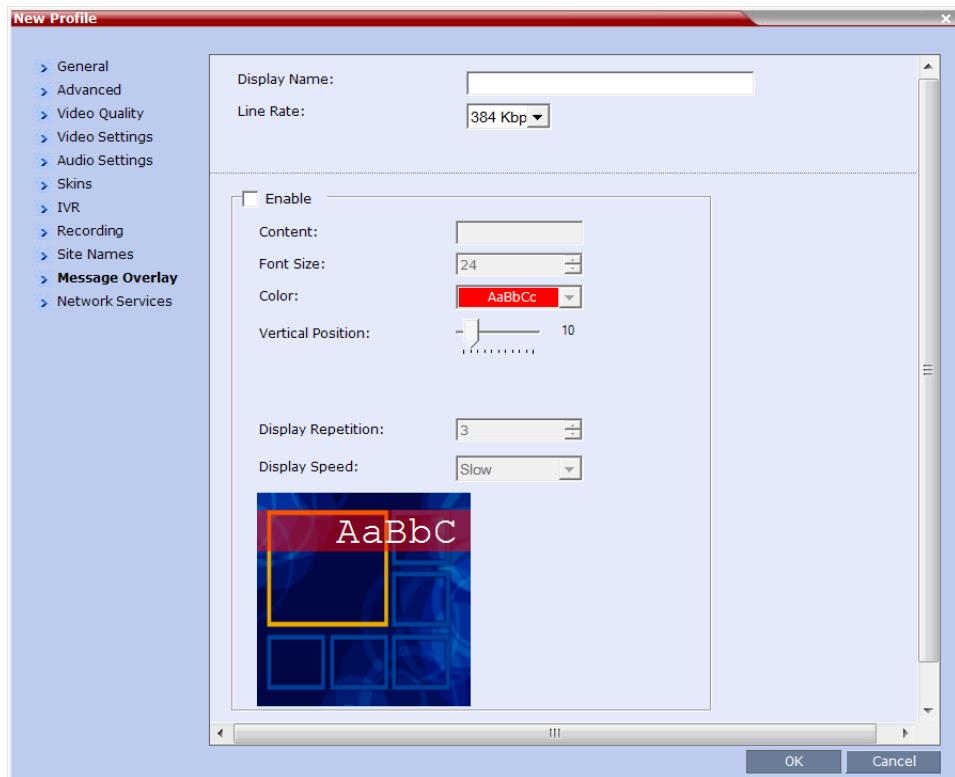
Message Overlay enables you to send text messages to all participants during ongoing Continuous Presence conferences.

The text message is seen as part of the in the participant's video layout on the endpoint screen or desktop display.

For more details, see "*Message Overlay for Text Messaging*" on page **2-33**.

Define the following fields:

Table 2-14 New AVC Profile - Message Overlay Parameters

Field	Description
Enable	Select this check box to enable *Message Overlay*. Clear this check box to disable *Message Overlay*. **Default:** Cleared. **Note:** • The *Message Overlay* field is shaded and disabled when *Video Switching* mode is selected in the *New Profile - General* tab. All other fields in this tab are also disabled. • Clearing the *Enable* check box enables *Video Switching* for selection in the *New Profile - General* tab. • If *Message Overlay* is selected, the *Video Switching* check box in the *New Profile - General* tab is disabled and cannot be selected.
Content	Enter the message text. The message text can be up to 50 Chinese characters.

Table 2-14 *New AVC Profile - Message Overlay Parameters (Continued)*

Field	Description
Font Size	Click the arrows to adjust the font size (points) for the *Message Overlay* display. **Range:** 9 - 32 **Default:** 24 **Note:** In some languages, for example Russian, when a large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.
Color	From the drop-down menu select the color and background of the *Message Overlay* display text. The choices are: AaBbCc **Default:** White Text on Red Background.
Vertical Position	Move the slider to the **right** to move the vertical position of the *Message Overlay* **downward** within the *Video Layout.* Move the slider to the **left** to move the vertical position of the *Message Overlay* **upward** within the *Video Layout.* **Default:** Top Left (10)
Display Repetition	Click the arrows to increase or decrease the number of times that the text message display is to be repeated. **Default:** 3
Display Speed	Select whether the text message display is static or moving across the screen, the speed in which the text message moves: • Static • Slow • Fast **Default:** Slow

As the fields are modified the *Preview* changes to show the effect of the changes.
For example:

Small Text, White on red, Top, Middle   *Small Text, White on yellow, Bottom*
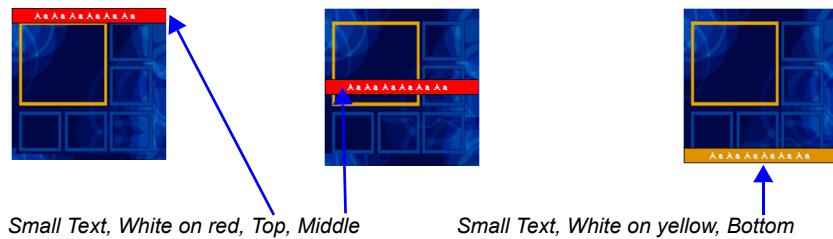
22 Click the **Network Services** tab.

The *New Profile - Network Services* tab opens.
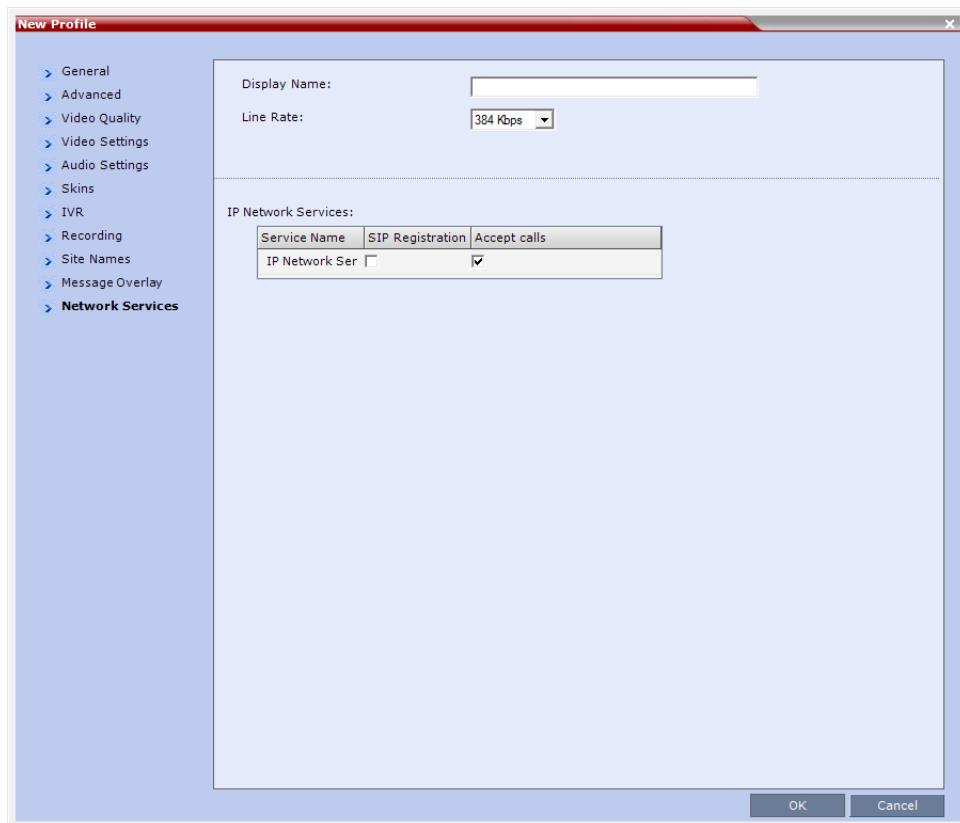
Registration of conferencing entities such as ongoing conferences, Meeting Rooms, Entry Queues, and SIP Factories with SIP servers is done per conferencing entity. This allows better control on the number of entities that register with each SIP server. Selective registration is enabled by assigning a conference Profile in which registration is configured to the required conferencing entities. Assigning a conference Profile in which registration is not configure to conferencing entities will prevent them from registering. By default, Registration is disabled in the Conference Profile, and must be enabled in Profiles assigned to conferencing entities that require registration.

23 Define the following parameters:

Table 2-15 *New AVC Profile - Network Services Parameters*

Parameter	Description
IP Network Services:	
Service Name	This column lists all the defined *Network Services,* one or several depending on the system configuration.
SIP Registration	To register the conferencing entity to which this profile is assigned with the SIP Server of the selected *Network Service*, click the check box of that *Network Service* in this column. When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with an URL derived from its own signaling address.
Accept Calls	To prevent dial in participants from connecting to a conferencing entity when connecting via a *Network Service*, clear the check box of the *Network Service* from which calls cannot connect to the conference.

24 Click **OK** to complete the *Profile* definition.
A new *Profile* is created and added to the *Conference Profiles* list.

CP Conferencing Additional Information

Overlay Layouts

Overlay Layouts allow additional participant endpoints to be displayed in 1x1 conference *Video Layout*s.

The following *Overlay Layouts* are available for use in *CP Conferences*:
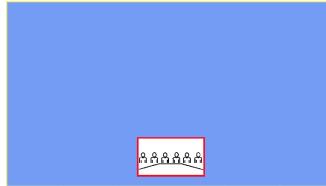
1Standalone Endpoint   **2 Standalone Endpoints**   **3 Standalone Endpoints**
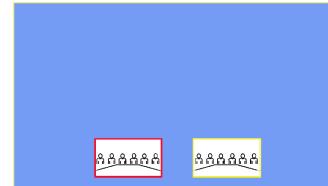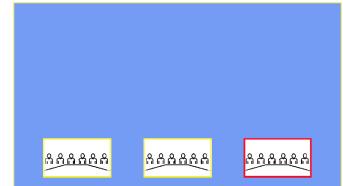
Although the following *Overlay Layout* is included in the *Profiles - Video Settings* dialog box it is not available for use in any conferencing mode:

Guidelines

• The *Overlay Layouts* are supported with both new and old *Skins* in *CP* mode. For more information see "*Skins*" on page **2-22**.

• The *Overlay Layouts* are 20% of the height of the endpoint display and are supported on endpoints of both 16:9 and 4:3 aspect ratios.

• *Overlay Layouts* are recommended for use with high resolution endpoints.

• *Message Overlay* is not affected by the use of *Overlay Layouts* and is displayed as the top level overlay.

• *Vertical Position* for *Site Name* display: *Site Names* are displayed for all cells. Because the smaller cells are located at the bottom of the large cell, when enabling *Site Names* it is advisable not to locate the *Site Name* at the bottom of the cells.

• *Standalone Endpoint Cells* are displayed each with a border. For all *Overlay Layouts,* border color is dependent on the selected *Skin*.
For more information see "*Skins*" on page **2-22**.

• System behavior for *Video Forcing* and *Personal Layout Control* using the *Overlay Layouts* during an ongoing conference is the same as for other video layouts.

• *Overlay Layouts* are only available for selection for the *Conference Layout* and are not available for selection for *Personal Layout*.

• *Overlay Layouts* are not available for selection when using *PCM* or *Click&View*.

• *PCM* menus are available when the *Overlay Layouts* are active, and they are displayed as the top level overlay

Selecting the Overlay Layouts

The *Overlay Layouts* are selected in the *New Profile - Video Settings* dialog box, in the *Overlay* tab of the *Video Layout* tree.

Not supported

Message Overlay for Text Messaging

Message Overlay allows the operator or administrator to send text messages to a single, several or all participants during an ongoing conference.

The text message is seen as part of the in the participant's video layout on the endpoint screen or desktop display.
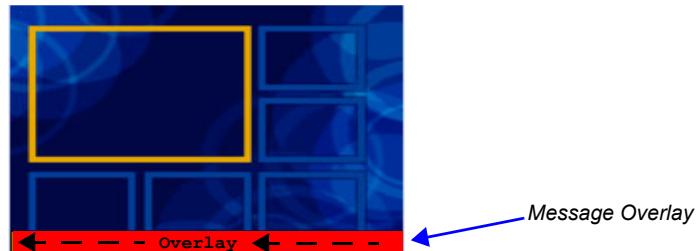
Message Overlay

Guidelines

- *Message Overlay* messaging is supported in:
    — in *Same Layout* mode
    — in encrypted conferences
- *Messages Overlay* can be enabled or disabled during the ongoing conference.
- *Message Overlay* text messages are supported in *Unicode* or *ASCII* characters.
- The number of characters for each language can vary due to the type of font used, for example, the available number of characters for Chinese is 32, while for English and Russian it is 48.
    — In some languages, for example Russian, when large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.
- Changes to the *Message Overlay* display characteristics (position, size, color and speed) are immediately visible to all participants.
- Changes to the *Message Overlay Content* are immediately visible to all participants. When there is a current *Message Overlay*:
    — The current message is stopped immediately.
    — The *Display Repetition* count is reset to 1.
    — The new message *Content* is displayed <*Display Repetition*> times or until it is stopped and replaced by another *Content* change.
- If a *Repeating Message* is modified before it has completed all its repetitions, it is changed immediately without completing all of its repetitions. The modified *Repeating Message* is displayed starting with repetition one.
- *Message Overlay* messaging is not supported in *Lecture* mode.
- If during the ongoing conference the **Show Number of Participants** DTMF option (default DTMF ***88**) is used, when the displayed number of participants is removed, the message overlay text is also removed.
- Participants that have their video suspended do not receive *Message Overlays* messages.
- *Message Overlay* text messages cannot be sent via the *Content* channel.
- *Message Overlay* messages are not displayed when the *PCM* menu is active.
- *Message Overlay* text settings are not saved in the *Conference Template* when saving an ongoing conference as a *Conference Template*.

Chinese Font Types

You can select one of several Chinese fonts for use when sending text over video. New fonts can be selected with the following features:

*   Site Names
*   Message Overlay
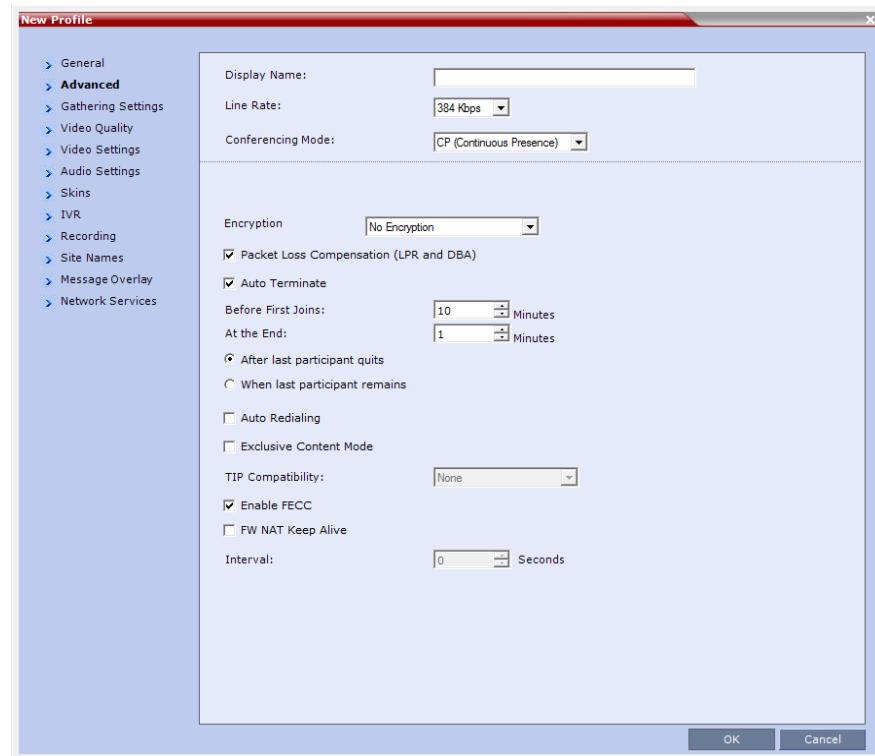
New Chinese fonts available are:

*   Heiti (Default)
*   Songti
*   Kaiti
*   Weibei

This feature has the following restrictions:

*   Available when either Simplified Chinese or Traditional Chinese is selected as an available language in **Setup > Customize Display Settings > Multilingual Setting**. The feature is hidden if neither Simplified Chinese nor Traditional Chinese is selected.
*   Only be accessed when using the RMX Web Client or the RMX Manager in Chinese.
*   Font cannot be changed during an existing conference. It can only be modified in a conference profile.
*   A participant moved to another conference will be shown the font used by the new conference, even if the conferences use different fonts.

Site Names Definition

Using the *Site Name* dialog box, you can control the display of the site names by defining the font, size, color, background color and transparency and position within the *Video Window*.

Site Names without Background (Plain Skin)

Site Names with Background (Picture Skin)
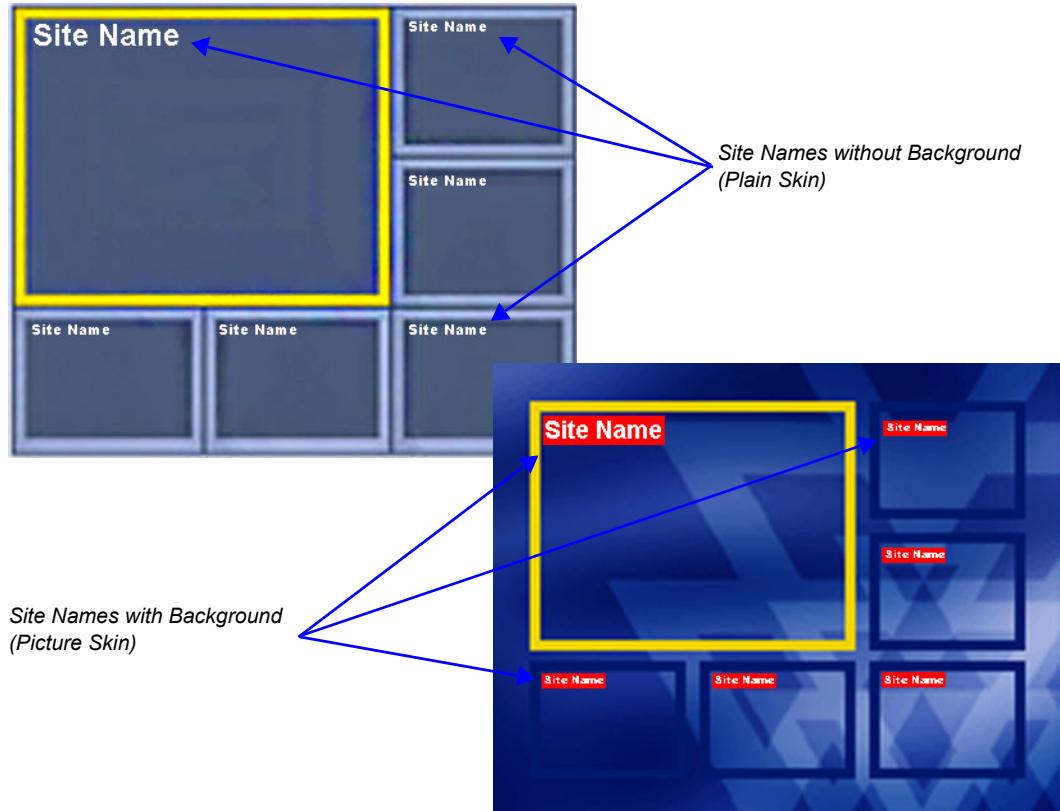
Guidelines

*   *Site Names* display is **Off** by default in a new profile.
*   *Site Names* can be enabled to function in one of two modes:
    — **Auto** – Site names are displayed for 10 seconds whenever the conference layout changes.
    — **On** – Site names are displayed for the duration of the conference.
*   During the display of the site names, the video frame rate is slightly reduced
*   *Site Names* display characteristics (position, size, color) can by modified during an ongoing conference using the *Conference Properties - Site Names* dialog box. Changes are immediately visible to all participants.
*   *Site Names* display text and background color is dependent on the *Skin* selected for the conference:
    — **Plain Skins** - *Site Names* text is displayed without a background.

— **Picture Skins** - *Site Names* text is displayed with a background.
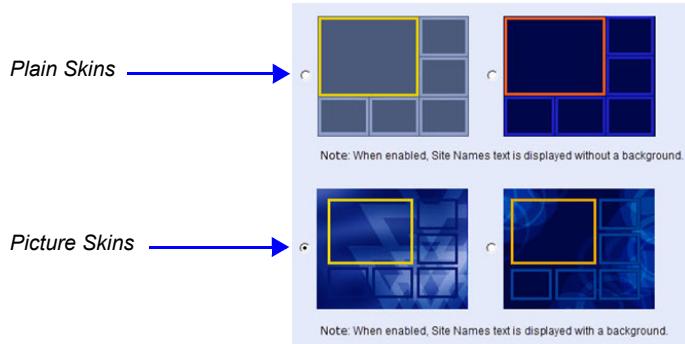
Plain Skins

Note: When enabled, Site Names text is displayed without a background.

Picture Skins

Note: When enabled, Site Names text is displayed with a background.

Exporting and Importing Conference Profiles

Conference Profiles can be exported from one MCU and imported to multiple MCUs in your environment, enabling you to copy the *Conference Profiles* definitions to other systems. This can save configuration time and ensures that identical settings are used for conferences running on different MCUs. This is especially important in environments using cascading conferences that are running on different MCUs.

Guidelines

*   Administrators can export and import *Conference Profiles*. Operators are only allowed to export *Conference Profiles*.
*   You can select a single, multiple, or all *Conference Profiles* to be exported.
*   *Conference Templates* and their related *Conference Profiles* can be exported and imported simultaneously using the *Conference Templates* export and import function. For more information, see the **Exporting and Importing Conference Templates** section.

Exporting Conference Profiles

Conference Profiles are exported to a single XML file that can be used to import the *Conference Profiles* on multiple MCUs.

Using the Export Conference Profile feature, you can:

*   Export all *Conference Profiles* from an MCU
*   Export selected *Conference Profiles*

Exporting All Conference Profiles from an MCU

To export all Conference Profiles from an MCU:

1   In the *RMX Management* pane, expand the *Rarely Used* list.

2   Click the **Conference Profiles** button.

The *Conference Profiles* are displayed in the *List* pane.

3 Click the **Export Conference Profiles** button or right-click the *Conference Profiles* pane, and then click **Export Conference Profiles**.

The *Conference Profile - Export* dialog box is displayed.

4 In the *Export Path* field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.

5 In the *Profiles file name* field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type *Profiles01*, the exported file name is defined as *Profiles01_confProfiles.xml*.

6 Click **OK** to export the *Conference Profiles* to a file.

If the export file with the same file name already exists, a prompt is displayed.
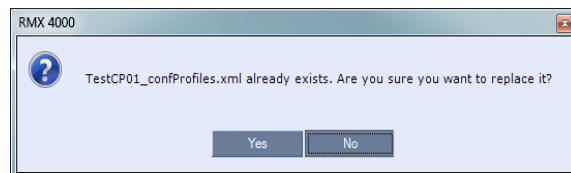
7 Click **Yes** to replace the exported file or click **No** to cancel the export operation and return to the *Conference Profiles* list. You can modify the export file name and restart the export operation.

Exporting Selected Conference Profiles

You can select a single Conference Profile or multiple Conference Profiles and export them to a file to be imported to other MCUs in your environment.

To export selected Conference Profiles:

1 In the *Conference Profiles* pane, select the profiles you want to export.

2 Right-click the selected *Conference Profiles,* and then click **Export Selected Conference Profiles**.
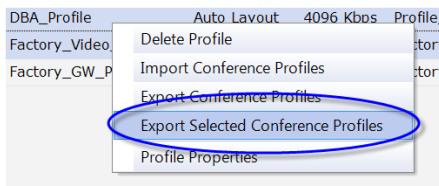
The *Conference Profile - Export* dialog box is displayed.
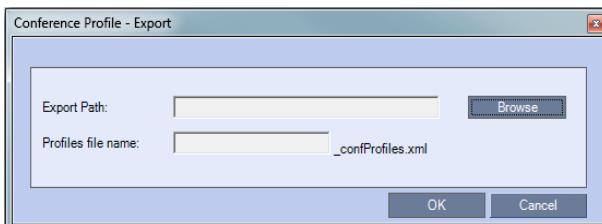
3 In the *Export Path* field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.

4 In the *Profiles file name* field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type *Profiles01*, the exported file name is defined as *Profiles01_confProfiles.xml*.

5 Click **OK** to export the *Conference Profiles* to a file.

If the export file with the same file name already exists, a prompt is displayed.
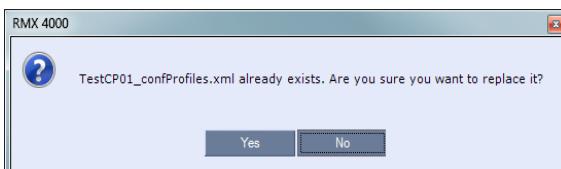
6 Click **Yes** to replace the exported file or click **No** to cancel the export operation and return to the *Conference Profiles* list. You can modify the export file name and restart the export operation.

Importing Conference Profiles

You can import Conference Profiles from another MCU in your environment.

To import Conference Profiles:

1 In the *RMX Management* pane, expand the *Rarely Used* list.

2 Click the **Conference Profiles** button.

The *Conference Profiles* are displayed in the *List* pane.

3   Click the **Import Conference Profiles** button or right-click the Conference Profiles pane, and then click **Import Conference Profiles**.

The *Conference Profile - Import* dialog box is displayed.
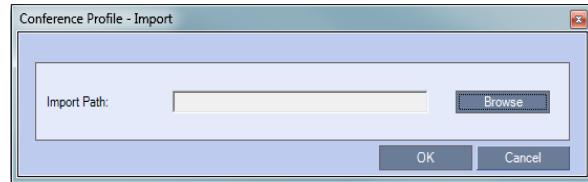
4   In the *Import Path* field, click **Browse** to navigate to the path and file name of the exported *Conference Profiles* you want to import.

5   Click **OK** to import the *Conference Profiles*.

Conference Profiles are not imported when:

—   A *Conference Profile* already exists

—   An IVR Service does not exist for the related *Conference Profile*

When *Conference Profiles* are not imported into the *Conference Profiles* list, a Message Alert window is displayed with the profiles that were not imported.
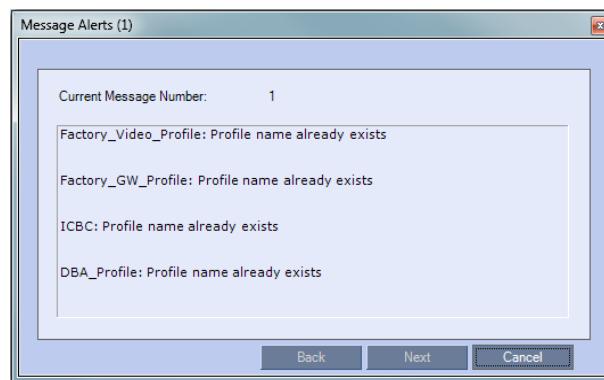
Conference Profiles that are not problematic are imported.

6   Click **Cancel** to exit the *Message Alerts* window.

The imported *Conference Profiles* appear in the *Conference Profiles* list.

Video Protocols and Resolution Configuration for CP Conferencing

Video Resolutions in AVC-based CP Conferencing

> The following video resolution information applies to AVC CP Conferencing Mode.

The *Polycom RMX 1800* always attempts to connect to endpoints at the highest line rate defined for the conference. If the connection cannot be established using the conference line rate, the Collaboration Server attempts to connect at the next highest line rate at its highest supported resolution.

Depending on the line rate, the Collaboration Server sends video at the best possible resolution supported by the endpoint regardless of the resolution received from the endpoint.

The video resolution is also defined by the *Video Quality* settings in the *Profile.*

*   **Motion**, when selected, results in lower video resolution at higher frame rates (30 fps to 60 fps).
*   **Sharpness**, when selected, results in higher video resolution at lower frame rate (30 fps and lower). However, it can also be sent in 1080P 60fps.

The combination of **frame rate** and **resolution** affects the number of video resources required on the MCU to support the call.

The following resolutions are supported:

*   CIF   352 x 288 pixels at 30 or 60 fps.
*   SD   720 x 576 pixels at 30 or 60 fps.
*   HD 720p   1280 x 720 pixels at 30 or 60 fps.
*   HD 1080p 1920 x 1080 pixels at 30 fps
*   HD 1080p 1920 x 1080 pixels at 60 fps (Symmetric in Motion and Sharpness)

Video Display with CIF, SD and HD Video Connections

Although any combination of CIF, SD and HD connections is supported in all CP conferences, the following rules apply:

*   In a 1X1 *Video Layout*:
    —   **SD:** If the speaker transmits CIF, the MCU will send CIF to all participants, including the SD participants. In any other layout the MCU will transmit to each participant at the participant's sending resolution.

— **HD:** The MCU transmits speaker resolution (including input from HD participants) at up to SD resolution. If 1x1 is the requested layout for the entire duration of the conference, set the conference to HD *Video Switching* mode.

- In asymmetrical *Video Layouts*:
    — **SD:** A participant in the large frame that sends CIF is displayed in CIF.
    — **HD:** Where participants' *video windows* are different sizes, the Collaboration Server transmits HD and receives SD or lower resolutions.
- In panoramic *Video Layouts*:
    — **SD**: Participants that send CIF also receive CIF.
    — **HD**: the Collaboration Server transmits HD and receives SD or lower resolutions, the Collaboration Server scales images from SD to HD resolution.

H.264 High Profile Support in CP Conferences

The *H.264 High Profile* is a new addition to the *H.264* video protocol suite. It uses the most efficient video data compression algorithms to even further reduce bandwidth requirements for video data streams.

Video quality is maintained at bit rates that are up to 50% lower than previously required. For example, a 512Kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.

H.264 High-Profile should be used when all or most endpoints support it.

Guidelines

- *H.264 High Profile* is supported in *H.323,* and *SIP* networking environments.
- *H.264 High Profile* is supported in *Continuous Presence* conferences at all bit rates, video resolutions and layouts.
- *H.264 High Profile* is the first protocol declared by the Collaboration Server, to ensure that endpoints that support the protocol will connect using it.

  Setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile*.
- For monitoring purposes, the Collaboration Server and endpoint *H.264 High Profile* capability is listed in the *Participant Properties - H.245* and *SDP* tabs for *H.323* participants and *SIP* participants respectively.
  For more information see "*IP Participant Properties"* on page .
- *H.264 High Profile* is not supported:
    — For *Content Sharing*
    — With *Video Preview*
- HD1080p 60 is supported in *Continuous Presence* (*CP*) mode:
    — In Motion Video Quality mode
    — With maximum bit rate of up to 4 Mbps
    — With a-symmetrical video qualities, the RMX receives HD720p60 and sends HD1080p60.
- PAL endpoints are supported at a frame rate of 50 fps.
- Each *HD1080p60* participant consumes 4 HD video resources.

- *HD1080p60* is not supported:
  — With *Content* sharing.

CP Conferencing with H.263 4CIF

The video resolution of 4CIF in H.263 endpoints is only supported for conferences in which the video quality is set to sharpness and for line rates of 384 Kbps to 1920 Kbps as shown in the following table.

Table 3-1   *Video Quality vs. Line Rate*

| Endpoint Line Rate Kbps | Video Quality | | | |
| | Motion | | Sharpness | |
	Resolution	Frame Rate	Resolution	Frame Rate
128	QCIF	30	CIF	30
256	CIF	30	CIF	30
384 - 1920+	CIF	30	4CIF	15

The Collaboration Server Web Client supports monitoring of H.263 4CIF information. The H.245 or SDP tab includes the additional information.

The creation of a new H.263 4CIF slide is supported in the IVR Service in addition to the current H.263 IVR slide. If users utilize the default Polycom slides that are delivered with the Collaboration Server, the slide's resolution will be as defined in the profile, i.e. SD, HD, CIF, etc.

For more information see "*High Resolution Slides*" on page **15-13**.

H.263 4CIF Guidelines

- H.263 4CIF is supported with H.323 and SIP connection endpoints.
- H.263 4CIF is supported in CP mode only.
- AES encryption is supported with H.263 4CIF.
- Recording of H.263 4CIF conferences is supported by the RSS 4000 and other devices.
- All video layouts are supported in H.263 4CIF, except 1x1 layout. In a 1x1 layout, the resolution will be CIF.
- H.239 is supported in H.263 4CIF and is based on the same bandwidth decision matrix as for HD.

The CP Resolution Decision Matrix

All the CP resolution options and settings are based on a decision matrix which matches video resolutions to connection line rates, with the aim of providing the best balance between resource usage and video quality at any given line rate.

The following factors affect the decision matrices:

- The used video protocol: *H.264 base Profile* or H.*264 High Profile*. The *H.264 High Profile* maintains the Video quality at bit rates that are up to 50% lower than previously

required. For example, a 512 kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.

- A different decision matrix is used for *Motion* and *Sharpness* as the quality requirements are different.

By default, the system shipped with three pre-defined settings of the decision matrix for H.264 *Base Profile* and three pre-defined settings of the decision matrix for *H.264 High Profile* with Motion and Sharpness video quality for each:

- **Resource-Quality Balanced (default)**

  A balance between video quality and resource usage. This is the only available resolution configuration in version 6.0.x and earlier.

- **Resource Optimized**

  System resource usage is optimized by allowing high resolution connections only at high line rates and may result in lower video resolutions (in comparison to other resolution configurations) for some line rates. This option allows to save MCU resources and increase the number of participant connections.

- **Video Quality Optimized**

  Video is optimized through higher resolution connections at lower line rates increasing the resource usage at lower line rates. This may decrease the number of participant connections.

Video Resource Usage

Video resource usage is dependent on the participant's line rate, resolution and *Video Quality* settings.

H.264 Base Profile and High Profile Comparison

The following illustrations show a comparison between the resolutions used at various line rates for H.264 baseline and the H.264 High Profile, for Motion and Sharpness Video Quality setting according to the *Resolution Configuration Mode* (*Balanced, Resource Optimized* or *Video Quality Optimized*).

H.264 Base Profile and High Profile Comparison - Sharpness

A comparison between the resolutions used at various line rates for *H.264 Baseline* and the *H.264 High Profile* for *Sharpness Video Quality* setting according to the following *Resolution Configuration Modes.*
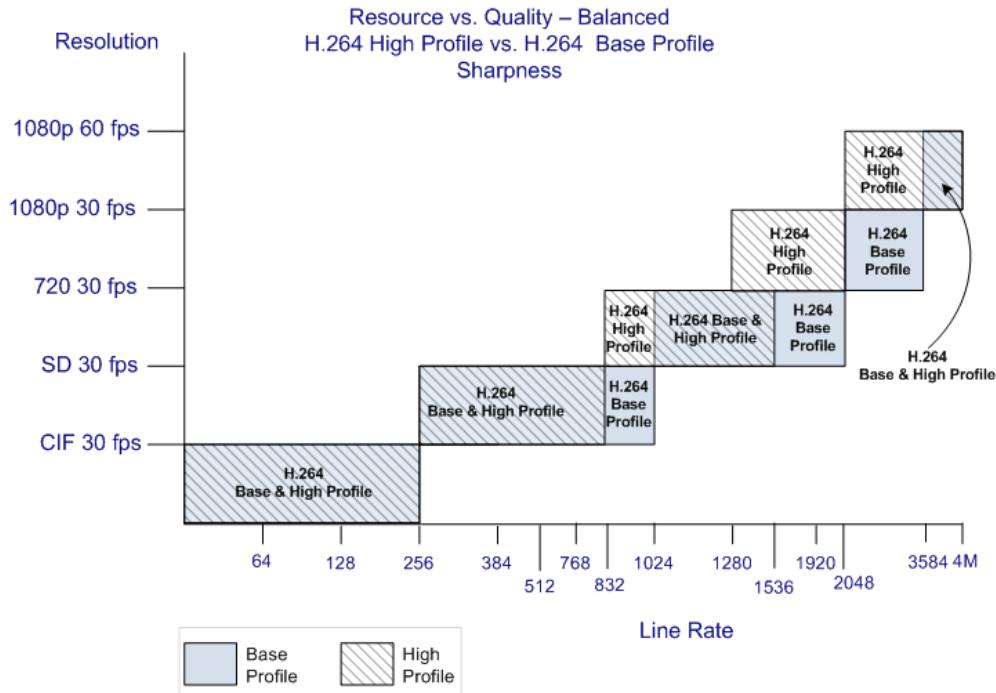
Figure 3-1 *Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Resource-Quality Balanced*
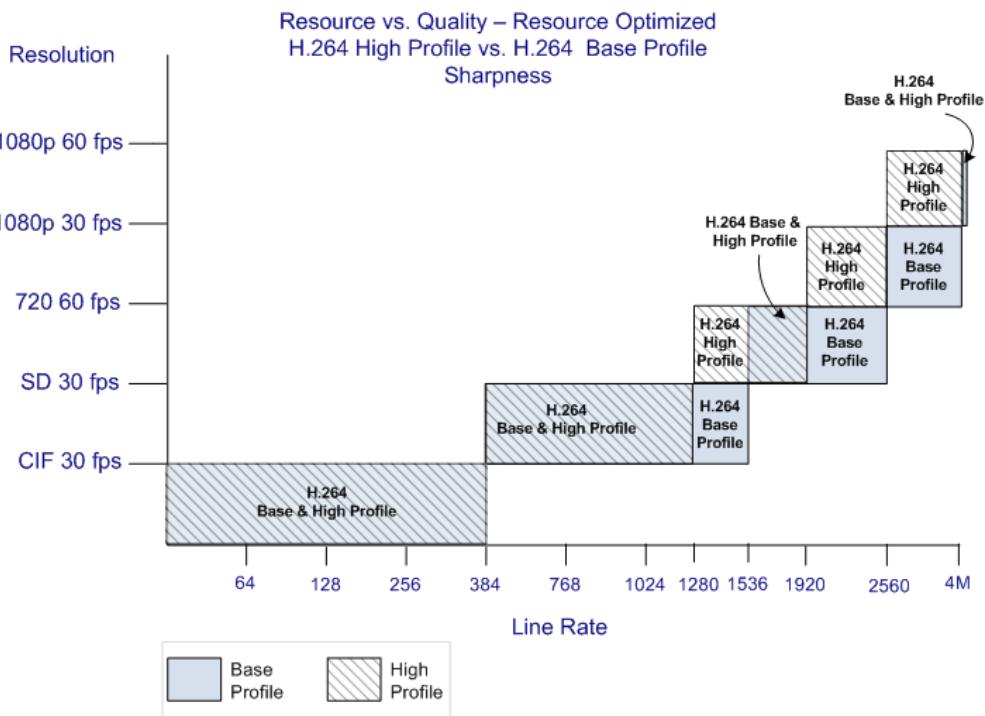
Figure 3-2 *Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Resource Optimized*
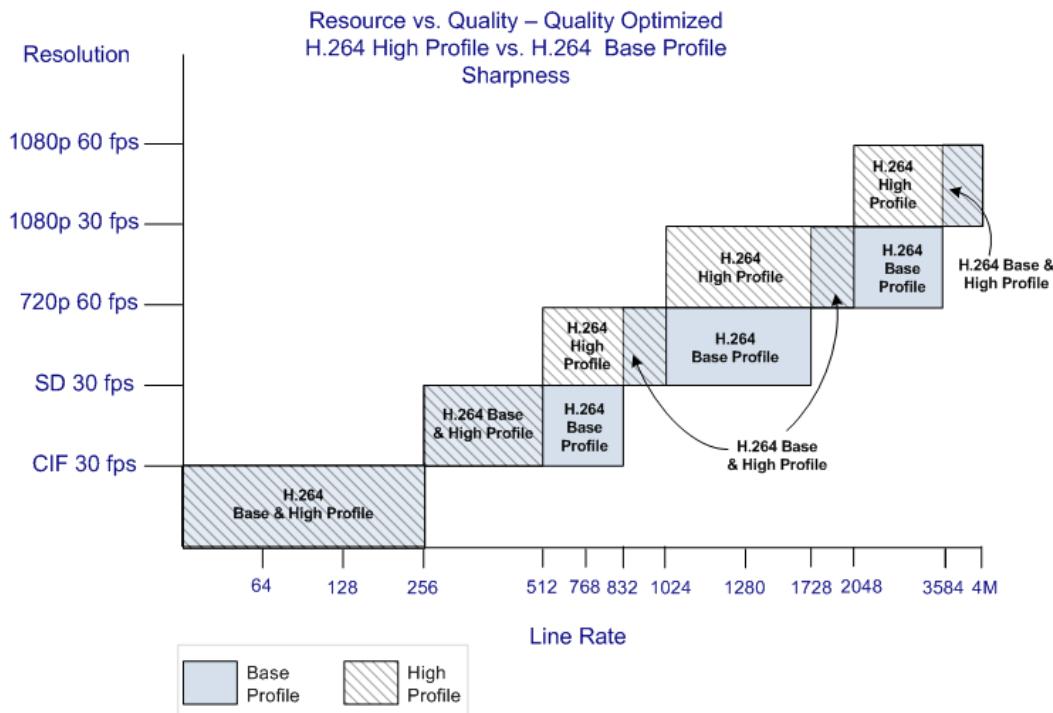
Figure 3-3 *Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Video Quality Optimized*

H.264 Base Profile and High Profile Comparison - Motion

A comparison between the resolutions used at various line rates for *H.264 Baseline* and the *H.264 High Profile* for *Motion Video Quality* setting according to the following *Resolution Configuration Modes.*
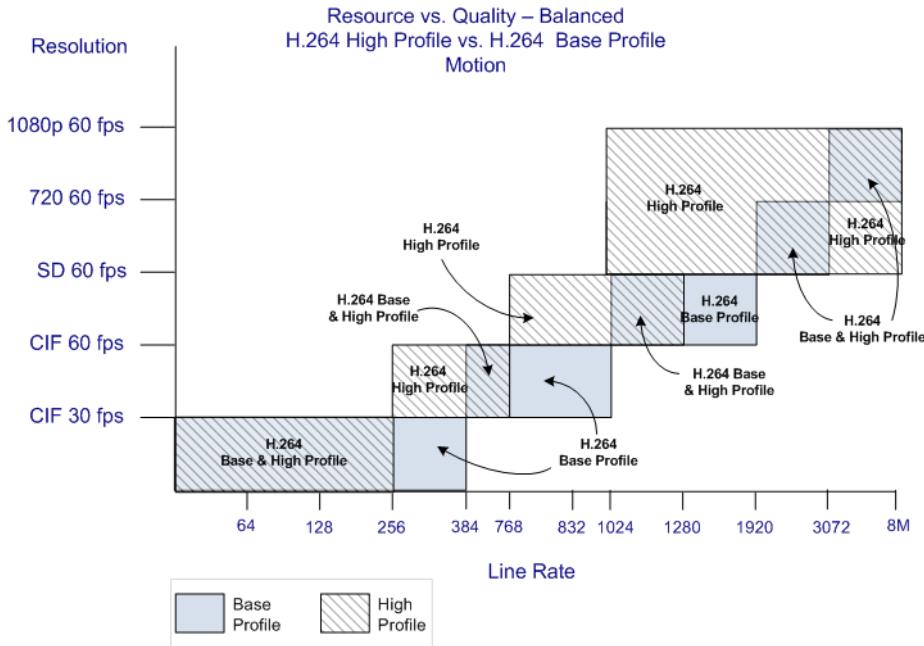
Figure 3-4 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource-Quality Balanced*
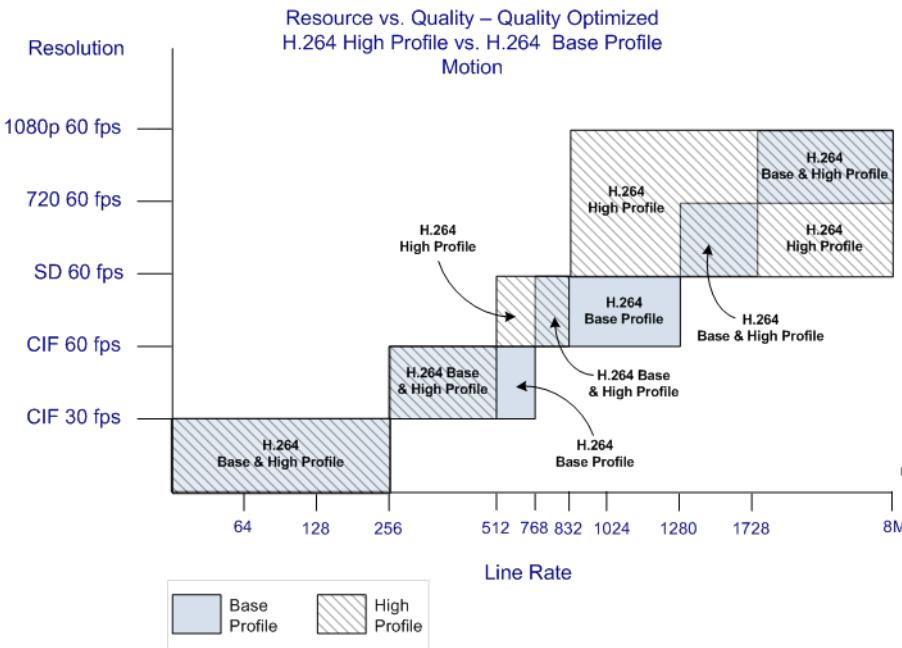
Figure 3-5 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Video Quality Optimized*
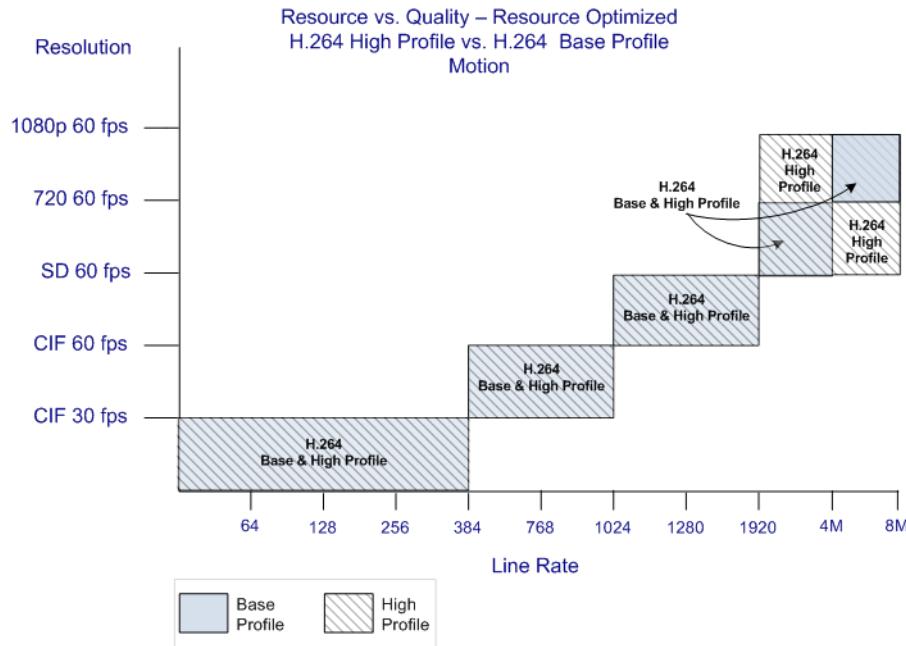
Figure 3-6 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource Optimized*

Default Minimum Threshold Line Rates and Resource Usage Summary

The following Table summarizes the *Default Minimum Threshold Line Rates* and *Video Resource* usage for each of the pre-defined optimization settings for each *Resolution*, *H.264 Profile*, *Video Quality* setting (*Sharpness* and *Motion).*

Table 3-2   *Default Minimum Threshold Line Rates and Video Resource Usage*

Resolution		Profile	Optimization Mode					
			Balanced		Resource		Video Quality	
			Sharpness	Motion	Sharpness	Motion	Sharpness	Motion
HD1080p60	Default kbps	High	2048	1728	2560	2560	2048	1472
		Base	3584	3072	4096	4096	3584	1728
HD1080p30	Default kbps	High	1536		4096		1024	
		Base	4096		4096		1728	
HD720p60	Default kbps	High		1280		1920		832
		Base		1920		1920		1280
HD720p30	Default kbps	High	832		1920		512	
		Base	1024		1920		832	
SD 60	Default kbps	High		768		1024		512
		Base		1024		1024		768
SD 30	Default kbps	High	256		384		256	
		Base	256		384		256	
CIF 60	Default kbps	High		256		384		256
		Base		384		384		256
CIF 30	Default kbps	High	64	64	64	64	64	64
		Base	64	64	64	64	64	64

The following table lists the resource capacity in various Polycom RMX 1800 configurations.

Resource Type/Video Resolution	3 Video Acceleration Cards	2 Video Acceleration Cards	1 Video Acceleration Card
Audio-only	100	100	100
H.261 CIF p30	50	35	15
H.263 CIF p30	100	70	35

Resource Type/Video Resolution	3 Video Acceleration Cards	2 Video Acceleration Cards	1 Video Acceleration Card
H.264 CIF p30	100	70	35
H.264 CIF p60	100	70	35
H.263 4CIF p30	100	70	35
H.264 4CIF p30	100	70	35
H.264 4CIF p60	100	70	35
H.264 720p30	100	70	35
H.264 720p60	50	35	17
H.264 1080p30	50	35	17
H.264 1080p60	25	17	8

Resolution Configuration for CP Conferences

The *Resolution Configuration* dialog box enables you to override the default video resolution decision matrix, effectively creating your own decision matrix. The minimum threshold line rates at which endpoints are connected at the various video resolutions can be optimized by adjusting the resolution sliders.

System resource usage is also affected by the *Resolution Configuration* settings. For more information see "*Video Resource Usage*" on page **3-4** and "*Default Minimum Threshold Line Rates and Resource Usage Summary*" on page **3-9**.

Guidelines

- *Resolution Slider* settings affect all *Continuous Presence* (*CP*) conferences running on the Collaboration Server. *Video Switched* conferences are not affected.
- A system restart is not needed after changing the *Resolution Slider* settings.
- *Resolution Slider* settings cannot be changed if there are ongoing conferences running on the Collaboration Server. .

Accessing the Resolution Configuration Dialog Box

The *Resolution Configuration* dialog box is accessed by clicking **Setup > Resolution Configuration** in the *Collaboration Server Setup* menu.

Modifying the Resolution Configuration

The *Resolution Configuration - Basic Configuration* dialog box is the first dialog box displayed .

Clicking the **Detailed Configuration** button toggles the display of the *Detailed Configuration* pane, which displays sliders for modifying minimum connection threshold line rates for endpoints that support *H.264 Base Profile* or *High Profile.* The *Detailed Configuration* pane can also be opened by clicking the **Manual** radio button in the *Resolution Configuration* pane.

Sharpness and *Motion* settings are accessed by clicking the **Sharpness** and **Motion** tabs when the *Detailed Configuration* is open.
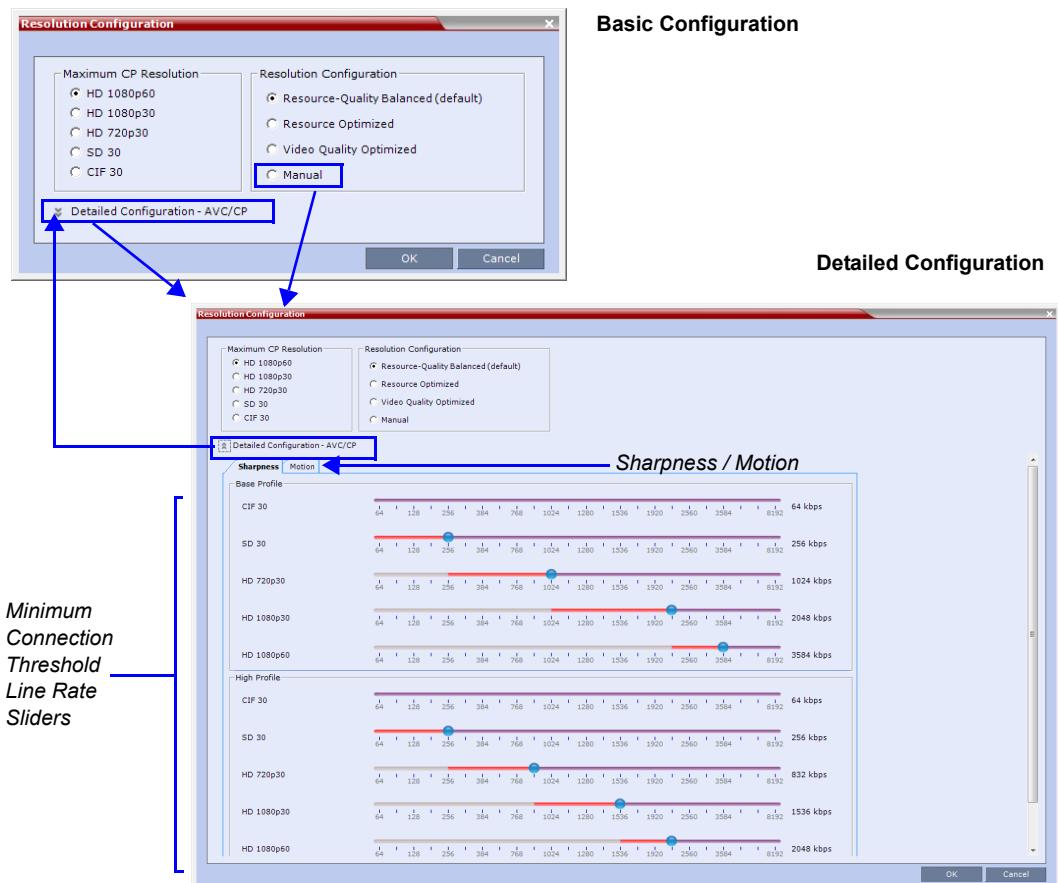
Resolution Configuration - Basic

The *Resolution Configuration -Basic* dialog box contains the following panes:

- *Max CP Resolution Pane*
- *Resolution Configuration Pane*

Maximum CP Resolution Pane

The Collaboration Server can be set to one of the following *Maximum CP Resolutions*:

- HD 1080p60
- HD 1080p30
- HD 720p30

- SD 30
- CIF 30

Limiting Maximum Resolution

Before a selection is made in this pane, the *Maximum CP Resolution* of the system is determined by the **MAX_CP_RESOLUTION** *System Flag*.
The **MAX_CP_RESOLUTION** flag value is applied to the system during *First Time Power-on* and after a system upgrade.

The default flag value is **HD1080** setting the *Maximum CP Resolution* value in the *Resolution Configuration* dialog box to 1**080p60**.

All subsequent changes to the *Maximum CP Resolution* of the system are made by selections in this pane.

The *Maximum Resolution* can further be limited per **conference** or per **participant endpoint**.

The *Maximum Conference Resolution*, can be limited via the *Profile - Video Quality* dialog box. For more information see "*Defining New Profiles"* on page **2-9**.

The *Maximum Resolution* can further be limited per participant endpoint via the *Participant - Properties* dialog box. For more information see "*Managing the Address Book"* on page **8-7**.

Resolution Configuration Pane

The user can select from 3 pre-defined *Resolution Configurations* or select a manual *Resolution Slider* adjustment mode. The pre-defined settings can be accepted without modification or be used as the basis for manual fine tuning of resolution settings by the administrator.

The *Manual* radio button is automatically selected if any changes are made to the *Resolution Sliders*.

The *Resolution Configurations* are:

- **Resource-Quality Balanced (default)**

  A balance between the optimized video quality and optimized resource usage.

Use this option:
- When the priority is to maintain a balance between resource usage and video quality.
- When it is necessary to maintain backward compatibility with previous versions.
- When working with Polycom DMA/RealPresence Resource Manager.

  The *Balanced* settings are described in the section*: "Default Minimum Threshold Line Rates and Resource Usage Summary"* on page **3-9**.

- **Resource Optimized**

  System resource usage is optimized by allowing high resolution connections only at high line rates and may result in lower video resolutions (in comparison to other resolution configurations) for some line rates.

Use this option when the priority is to save MCU resources and increase the number of participant connections.

  The *Resource Optimized* settings are described in the section*: "Default Minimum Threshold Line Rates and Resource Usage Summary"* on page **3-9**.

- **Video Quality Optimized**

  Video is optimized through higher resolution connections at lower line rates increasing the resource usage at lower line rates. This may decrease the number of participant connections.

> Use this option when the priority is to use higher video resolutions while decreasing the number of participant connections.

The V*ideo Quality Optimized* settings are described in the section*: "Default Minimum Threshold Line Rates and Resource Usage Summary"* on page **3-9**.

- **Manual**

  Manually adjusting the sliders to accommodate local conferencing requirements.

Resolution Configuration - Detailed

H.264 High Profile allows higher quality video to be transmitted at lower bit rates.

However, setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile*. The Collaboration Server uses two decision matrices (*Base Profile*, *High Profile)* to enable endpoints to connect according to their capabilities.

Sharpness and Motion

Sharpness and *Motion* are *Video Quality* settings that are selected per conference and are defined in the conference *Profile.* A conference with *Sharpness* selected in its *Profile* uses the *Sharpness* settings of the *Resolution Configuration* and a conference with *Motion* selected in its *Profile* uses the *Motion* settings of the *Resolution Configuration* dialog box.

The *Sharpness* and *Motion* tabs in the *Resolution Configuration* dialog box allow you to view and modify *Resolution Configuration* settings for conferences with either *Video Quality* setting.

Resolution Configuration Sliders

The *Detailed Configuration* dialog box allows you to configure minimum connection threshold bit rates for endpoints that support *H.264 High Profile* and those that do not support *H.264 High Profile* by using the following slider panes:

- *Base Profile* - Endpoints that do not support *H.264 High Profile* connect at these minimum threshold bit rates.
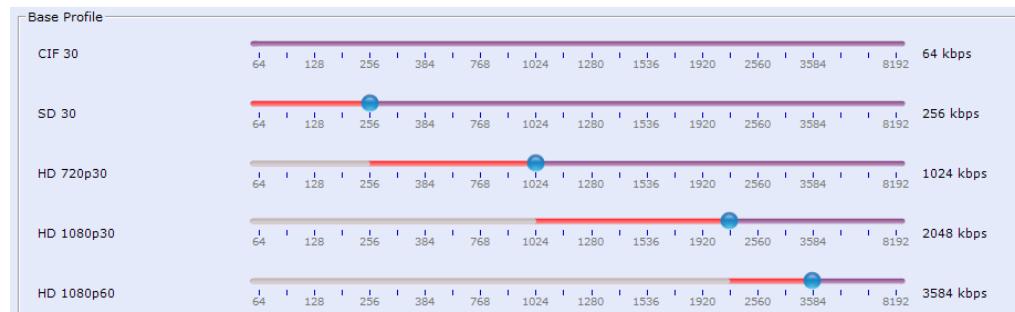
- *High Profile* - Endpoints that support *H.264 High Profile* connect at these minimum threshold bit rates.
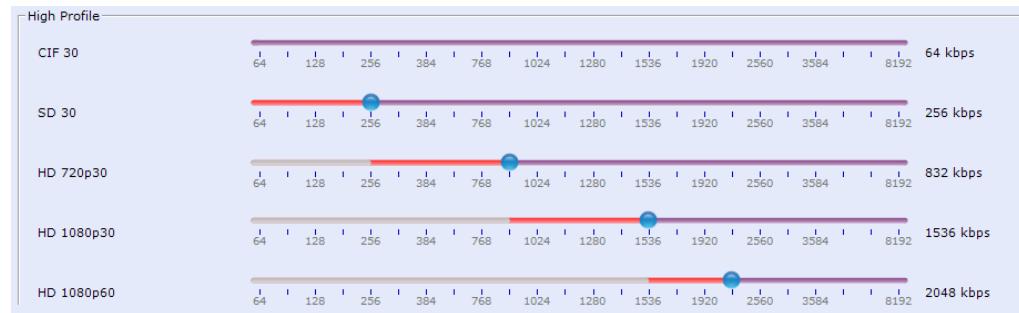
Although the default minimum threshold bit rates provide acceptable video quality, the use of higher bit rates usually results in better video quality but will require more resources.

The *Base Profile* and *High Profile* sliders operate in the same manner in *Sharpness* and in *Motion*.

Video Resource usage is affected by the *Resolution Configuration* settings. The lower the line rate threshold set for a certain resolution the more resources will be used to connect that participant (as a higher resolution will be used).

Moving the slider of a certain resolution to the left reduces the line rate threshold required for the endpoints to connect using that resolution (resulting in higher video quality, more video resources). Moving the slider to the right, increases the line rate required for the endpoint to connect using that resolution (resulting in lower video quality, less video resources).

The following example demonstrate the usage of the sliders.

- Moving the *HD720p30* resolution slider from 1024kbps to 1920kbps increases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 1024kbps and 1920kbps that would have connected at *HD 720p30* resolution will instead connect at *SD 30* resolution. Each of the affected endpoints will connect at lower resolution but will use less video resources.

- Moving the *HD1080p60* resolution slider from 3584kbps to 2560kbps decreases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 2560kbps and 4096kbps that would have connected at *HD 1080p30* resolution will instead connect at *HD 1080p60* resolution. Each of the affected endpoints will connect at higher resolution but will use more video resources.

Flag Settings

Setting the Maximum CP Resolution for Conferencing

The **MAX_CP_RESOLUTION** flag value is applied to the system during *First-time Power-up* and after a system upgrade. The default value is *HD1080*.

All subsequent changes to the *Maximum CP Resolution* of the system are made by selections in the *Max CP Resolution* pane of the **Resolution Configuration** dialog box.

Minimum Frame Rate Threshold for SD Resolution

The **MINIMUM_FRAME_RATE_THRESHOLD_FOR_SD** *System Flag* can be added and set to prevent low quality, low frame rate video from being sent to endpoints by ensuring that an *SD* channel is not opened at frame rates below the specified value. For more information see "*Modifying System Flags*" on page **20-1**.

Additional Video Resolutions

The following higher video quality resolutions are available with the Collaboration Server

- CIF 352 x 288 pixels at 50 fps.
- WCIF   512 x 288 pixels at 50 fps.
- WSD   848 x 480 pixels at 50 fps.
- W4CIF   1024 x 576 pixels at 30 fps.
- HD 720p   1280 x 720 pixels at 60 fps.
- HD 1080p 1920 x 1080 pixels at 30 fps.
- HD 1080p 1920 x 1080 pixels at 60 fps.

Two higher quality, intermediate video resolutions replace the transmission of CIF (352 x 288 pixels) or SIF (352 x 240 pixels) resolutions to endpoints that have capabilities between:

- **CIF** (352 x 288 pixels) and **4CIF** (704 x 576 pixels) – the resolution transmitted to these endpoints is **432 x 336** pixels.
- **SIF** (352 x 240 pixels) and **4SIF** (704 x 480 pixels) – the resolution transmitted to these endpoints is **480 x 352** pixels.

4

Additional Conferencing Information

Various conferencing modes and video features require additional settings, such as system flag settings, conference parameters and other settings. In depth explanations of these additional settings are described in the following sections:

Content Sharing

Content such as graphics, presentations, documents or live video can be shared with conference participants using the H.239 (H.323) or BFCP (SIP) protocol, which is the standard protocols for content sharing.

H.239 Protocol

The *H.239* protocol allows compliant endpoints to transmit and receive two simultaneous video streams:

- **People video stream** – video is displayed in Continuous Presence conferences
- **Content video stream** – Video Switching mode for content sharing

By default, all conferences, *Entry Queue*s, and *Meeting Rooms* launched on the *Collaboration Server* have *H.239* capabilities.

To view *Content*, endpoints must use the same Bit Rate, Protocol, and Resolution. Endpoints may not send *Content* while connecting to an *Entry Queue*.

Endpoints without *H.239* capability can connect to the video conference without *Content*.

Cascade links declare *H.239* capabilities and they are supported in *Star* cascading topologies. For more details, see .

SIP BFCP Content Capabilities

SIP Clients supporting *BFCP* over *UDP,* when connected to conferences on the Collaboration Server, can share *Content* with endpoints supporting the following *Content* sharing protocols:

*   *BFCP/TCP*
*   *BFCP/UDP*
*   *H.323/ H.239*

Guidelines:

For *SIP Clients* that support both *BFCP/TCP* and *BFCP/UDP*:

*   The preferred protocol is *BFCP/UDP*.
*   When used in *Cascading* conferences, the *Cascade Link* must be *H.323*.
*   *BFCP/UDP* is supported in both *IPv4* addressing modes.
*   *BFCP* utilizes an unsecured channel (port 60002/ TCP) even when *SIP TLS* is enabled. *BFCP* capabilities are by default declared to all endpoints. If, however, the endpoint identity is hidden by a proxy server, these capabilities will not be declared by the Collaboration Server. Capabilities declaration is controlled by the **ENABLE_SIP_PPC_FOR_ALL_USER_AGENT** *System Flag*.

    The default value of the **ENABLE_SIP_PPC_FOR_ALL_USER_AGENT** *System Flag* is **YES** resulting in *BFCP* capability being declared with all vendors' endpoints unless it is set to **NO**. When set to **NO**, the Collaboration Server will declare *BFCP* capabilities to *Polycom* and *Avaya* endpoints.

*   The **ENABLE_FLOW_CONTROL_REINVITE** *System Flag* should be set to **NO** when *SIP BFCP* is enabled.
*   If these *System Flags* don't exist in the system, they must be manually added. For more information see "*Modifying System Flags"* on page **20-1**.
*   BFCP capabilities are not supported in Microsoft ICE environment.

Dial-out Connections:

*   For dial-out connections to *SIP Clients*, *BFCP/UDP* protocol can be given priority by adding the adding the **SIP_BFCP_DIAL_OUT_MODE** *System Flag* to *system.cfg* and setting its value to UDP.

    The *Collaboration Server' s Content* sharing determined by the *System Flag's* settings and *SIP Client* capabilities are summarized in Table 4-1.

Table 4-1   System Flag - SIP_BFCP_DIAL_OUT_MODE

Flag Value	SIP Client: BFCP Support		
	UDP	**TCP**	**UDP and TCP**
AUTO (Default)	BFCP/**UDP** selected as *Content* sharing protocol.	BFCP/**TCP** selected as *Content* sharing protocol.	BFCP/**UDP** selected as *Content* sharing protocol.
UDP		Cannot share *Content*.	

Table 4-1   *System Flag - SIP_BFCP_DIAL_OUT_MODE*

Flag Value	SIP Client: BFCP Support		
	UDP	TCP	UDP and TCP
TCP	Cannot share *Content*.	BFCP/**TCP** selected as *Content* sharing protocol.	

For more information see "*Manually Adding and Deleting System Flags"* on page **20-10**.

Dial-in Connections:

• The Collaboration Server will share content with *Dial-in SIP Clients* according to their preferred *BFCP* protocol.

• *SIP Clients* connected as *Audio Only* cannot share *Content*.

Defining Content Sharing Parameters for a Conference

Content can be shared using two main methods:

• Content Highest common parameters (also known as Content Video Switching)

• Multiple Content Resolutions

In *Content Video Switching* mode, the content is negotiated to highest common capabilities supported by the endpoints connected to the conference. If the conference includes participants that support lower content capabilities (such as H.263) and higher content capabilities (H.264), content will be sent at the lower capabilities supported by all endpoints, resulting in lower content quality seen by all endpoints.

In this mode, the content is set according to the capabilities of all the participants currently connected to the conference. If the all the connected participant support the H.264 protocol, the Content will be started with H.264 capabilities. If then an endpoint supporting only H.263 protocol connects, the content is stopped in order to switch to H.263 and has to be resent. If the H.263 participant leaves the conference and only H.264 capable endpoints remain connected, content is stopped in order to switch back to H.264 and has to be resent.

In *Multiple Content Resolutions* mode*, c*ontent is shared in multiple streams, one for each video protocol: H.263 and H.264. A separate video resource is used to process the *Content* shared with H.264-capable endpoints and another for content shared with H.263-capable endpoints, with each endpoint receiving its highest possible quality. This allows endpoints with different protocols to connect and disconnect without having to restart *Content* sharing in the middle of a conference.

In this mode, endpoints that do not support the content capabilities set for the conference will receive the content over the video (people) channel ("Legacy" content).

Content parameters are defined in the *Conference Profiles - Video Quality* dialog box.
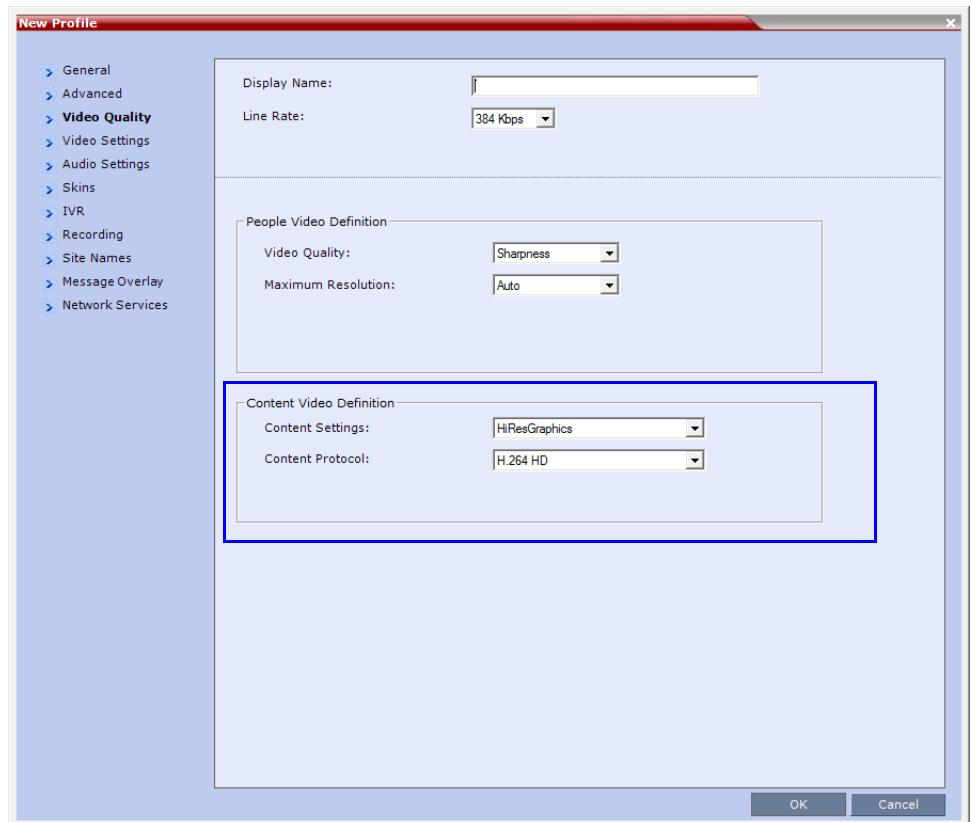
1   In the *Content Video Definition* section, select the *Content Settings* and *Protocol* as follows:

Table 4-2   *H.239 Content Options*

Field	Description
Content Settings	Select the transmission mode for the Content channel: • **Graphics** — basic mode, intended for normal graphics • **Hi-res Graphics** — a higher bit rate intended for high resolution graphic display • **Live Video** — Content channel displays live video • **Customized Content Rate** - manual definition of the Conference Content Rate, mainly for cascading conferences. Selection of a higher bit rate for the *Content* results in a lower bit rate for the people channel. For a detailed description of each of these options, see "*Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode*" on page **4-5**.
AS-SIP Content	This Content Sharing option is not supported with Polycom RMX 1800.

Table 4-2 *H.239 Content Options (Continued)*

Field	Description
Multiple Resolutions	This Content Sharing option is not supported with Polycom RMX 1800.

Content Protocol	• **H.263**
	  • *Content* is shared using the *H.263* protocol.
	  • Use this option when most of the endpoints support *H.263* and some endpoints support *H.264*.
	• **H.263 & H.264 Auto Selection** ()
	  • *Content* is shared using *H.263* if a mix of H.263-supporting and *H.264*-supporting endpoints are connected.
	  • *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
	• **H.264 HD** default
	  • Ensures high quality *Content* when most endpoints support *H.264* and *HD Resolutions*.
	• **H.264 Cascade and SVC Optimized**
	  • All *Content* is shared using the *H.264* content protocol and is optimized for use in *Cascaded Conferences*.
	For a detailed description of each of these settings, see "*Content Protocols*" on page **4-7**.

Content Resolution	Select a *Content Resolution* from the drop-down menu. The *Content Resolutions* that are available for selection are dependent on the content sharing mode (Highest Common Content or Multiple Content Resolutions), *Line Rate* and *Content Settings* that have been selected for the conference. For a full list of *Content Resolutions* see "*Defining Content Sharing Parameters for a Conference*" on page **4-3**. **Note:** This field is displayed only when **H.264 Cascade** *is selected for Multiple Content Resolution or when* **H.264 Cascade and SVC Optimized** option is selected as the *Content Protocol* (in the Highest Common Content Mode) and is enabled for selection in CP conferences.
Send Content to Legacy Endpoints	This Content Sharing option is not supported with Polycom RMX 1800.

2   Click **OK.**

Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode

This section describes the possible content sharing parameters when content Highest Common mode is used:

• Content Settings
• Content Protocol

- Content Resolution

Content Settings

The Content channel can transmit one of the following modes:

- **Graphics** – for standard graphics.
- **Hi-res Graphics** – requiring a higher bit rate, for high quality display or highly detailed graphics.
- **Live Video** – highest bit rate, for video clips or live video display.
- **Customized Content Rate** - that allows manual definition of the *Conference Content Rate*.

Content Setting

For *Graphics*, *Hi-res Graphics* and *Live Video*, the highest common Content bit rate is calculated for the conference each time an endpoint connects. Therefore, if an endpoint connects to an ongoing conference at a lower bit rate than the current bit rate, the Content bit rate for the current conference is re-calculated and decreased.

Bit rate allocation by the MCU is dynamic during the conference and when the Content channel closes, the video bit rate of the *People conference* is restored to its maximum.

During a conference the MCU will not permit an endpoint to increase its bit rate, it can however change its Content resolution. The Collaboration Server can decrease the allocated Content bit rate during a conference.

The following table summarizes the bit rate allocated to the Content channel from the video channel in each of the *Content Settings* according to the conference line rate:

Table 4-3 Decision Matrix - Bit Rate Allocation to Content Channel per Conference Line Rate

Content Settings	Content Bit Rate Allocation per Conference Line Rate (kbps)											
	64 96	128	256	384	512	768 832	1024 1152	1472 1728	1920	2048	4096	6144
Graphics		64	64	128	128	256	256	256	256	256	256	1536
Hi Resolution Graphics		64	128	192	256	384	384	512	768	768	1536	1536
Live Video		64	128	256	384	512	768	768	1152	1152	1536	1536
Customized Content Rate	The Content Bit Rate is selected from a menu in the *Content Video Definition* pane. See "*Selecting a Customized Content Rate"* on page **4-13**.											

Table 4-4   *Decision Matrix - Bit Rate Allocation to Content Channel per Conference Line Rate*

Content Settings	Content Bit Rate Allocation per Conference Line Rate (kbps)								
	64 96	128	256	384	512	768 832	1024 1152	1472 1728	1920
Graphics		64	64	128	128	256	256	256	256
Hi Resolution Graphics		64	128	192	256	384	384	512	768
Live Video		64	128	256	384	512	768	768	1152
Customized Content Rate	The Content Bit Rate is selected from a menu in the *Content Video Definition* pane. See "*Selecting a Customized Content Rate"* on page **4-13**.								

Table 4-5 summarizes the *Maximum Resolution* of *Content* and *Frames per Second (fps)* for *Bit Rate Allocations* to the *Content Channel*.

Table 4-5   *Content - Maximum Resolution, Frames/Second per Bit Rate Allocation*

Bit Rate Allocated to Content Channel (Kbps)	Content	
	Maximum Resolution	**Frames/Second**
*From **64** and less than **512***	H.264 HD720p	5
*From **512** and up to **768***	H.264 HD720p	30
*From **768** and up to **1536***	H.264 HD1080p	15

Content Protocols

Two *Content Protocols* can be used for sharing content:

• H.263

• H.264

H.264 offers higher quality content, but is not supported by legacy endpoints. Depending on the endpoints capabilities, you can determine the content sharing experience by selecting the appropriate protocol and system behavior from the *Content Protocol* list:

• *H.263 & H.264 Auto Selection*

• *H.263*

• *H.264 HD*

• *H.264 Cascade and SVC Optimized*

H.263 & H.264 Auto Selection ()

The **H.263 & H.264 Auto Selection** option should be selected when *Content* is to be shared using a mix of *H.263*-supporting and *H.264*-supporting endpoints.

Bit rate allocation to the *Content* channel by the Collaboration Server is dynamic according to the conference line rate and *Content Setting* selected for the conference.

If an endpoint that supports only *H.263* for Content Sharing connects to a conference with Content Protocol set to *H.263 & H.264 Auto Selection*:

- *Content* is shared using *H.263* even if *H.264*-supporting endpoints are connected.
- *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
- If the first endpoint to connect to the conference only supports *H.263,* the *H.263* protocol is used for *Content* for all conference participants.
- If *Content* is already being shared using the *H.264* protocol when a *H.263* endpoint connects, *Content* sharing is stopped and must be manually restarted using *H.263* (i.e. the endpoint using H.263 Content Protocol must connect first), for all participants to receive content. If the *H.263* endpoint disconnects, *Content* sharing must be manually stopped and restarted and will automatically upgrade to the *H.264* protocol.
- Endpoints that do not have at least *H.263* capability can connect to the conference but cannot share *Content*.

H.263

Select this option when most of the endpoints support *H.263* and some endpoints support *H.264*. In such a case, all endpoints will share content using the H.263 protocol, and this protocol will not change throughout the conference (fixed mode).

Bit rate allocation to the *Content* channel by the Collaboration Server is dynamic according to the conference line rate and *Content Settings* selected for the conference. For more information see "*Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode"* on page **4-5**.

H.264 HD default

The **H.264 HD** option should be selected only if most endpoints in the conference support *H.264* to ensure high quality *Content*.

When this protocol option is selected, endpoints must connect at *Content* bit rates above a minimum as specified by specific *System Flags* to ensure high quality *Content* for all participants. For more information about *System Flags* see "*Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD"* on page **4-9**.

Bit rate allocation to the *Content* channel by the Collaboration Server is dynamic according to the conference line rate and *Content Setting* selected for the conference. For more information see "*Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode"* on page **4-5**.

Endpoints that do not support *H.264*, or those that do not meet the minimum line rate threshold for the *Content Setting* will not receive content.

Guidelines

- Only endpoints that support *H.264* capability at a resolutions of *HD720p5* or higher will be able to receive and send *Content*.
- The minimum *Content Rate* required for allowing a participant to share *Content* is the lower valued parameter when comparing the *System Flag* setting *(*Table 4-6*)* and the *content bit rate allocation* derived from the conference line rate.

  When the flag settings enable an endpoint to share Content at a content rate that is lower than the conference content rate, the content rate of the entire conference is reduced to the content rate supported by that endpoint.

Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD

The following *System Flags* determine the minimum content rate required for endpoints to share *H.264* high quality content via the *Content* channel.

A *System Flag* determines the minimum line rate for each *Content Setting*:

*   *Graphics*
*   *Hi Resolution Graphics*
*   *Live Video*

In order to change the *System Flag* values, the flags must be manually added to the *System Configuration*. For more information see "*Modifying System Flags*" on page **20-1**.

Table 4-6   H.264 HD System Flags

Content Settings	Flag Name	Range	Default
Graphics	*H264_HD_GRAPHICS_MIN_CONTENT_RATE*	0-1536	128
Hi Resolution Graphics	*H264_HD_HIGHRES_MIN_CONTENT_RATE*	0-1536	256
Live Video	*H264_HD_LIVEVIDEO_MIN_CONTENT_RATE*	0-1536	384

Example

Table 4-7 summarizes an example of two participants trying to connect to a conference running at a *Line Rate* of 1024Kbps. The *Content Setting* for the conference is **Hi Resolution Graphics** and the **H264_HD_HIGHRES_MIN_CONTENT_RATE** *System Flag* setting are used to determine if *Content* will be shared with the participant.

Table 4-7   *Participant Content Sharing Based on Connection Line Rate and System Flag Setting*

		Participant		Conference			
		Line Rate	Bit Rate Allocation to Content Channel (Table 4-5)	Line Rate	Bit Rate Allocation to Content Channel (Table 4-5)	Flag Value	Result
Participant 1		384	192	1024	384	128	Participant and entire conference share content at 192Kbps
						512	Participant will not receive content
Participant 2		1024	384			128	Participant and entire conference share content at 384Kbps
						512	Participant and entire conference share content at 384Kbps

H.264 Cascade and SVC Optimized

The **H.264 Cascade and SVC Optimized** option maintains content quality and minimizes the amount of content refreshes that occur in large cascading conferences when participants connect or disconnect from the conference.

In AVC CP conferences, each content *Line Rate* and *Content Setting* has its own resolution and frame rate.

In AVC CP conferences, endpoints that do not support the required content parameters (*Content* line rate, *H.264* protocol and *Content Resolution)*, will not receive content.

Endpoints that do not support the required content parameters (*Content* line rate and *Content Resolution)* cannot share content.

Guidelines

• In Cascading conferences, the cascade link must be *H.323.*

• *H.264 High Profile* is not supported.

Enabling H.264 Cascade and SVC Optimized Content Sharing in AVC CP Conferences

When *H.264 Cascade and SVC Optimized* is selected as the *Content Protocol*, an additional field, *Content Resolution* is displayed in the *Content Video Definition* pane.

The *Content Resolution* is a fixed resolution and frame rate for *Content* sharing in a Cascaded Conference. The *Content Resolution* that are available for selection are dependent on the *Line Rate* and *Content Settings* that have been selected for the conference.
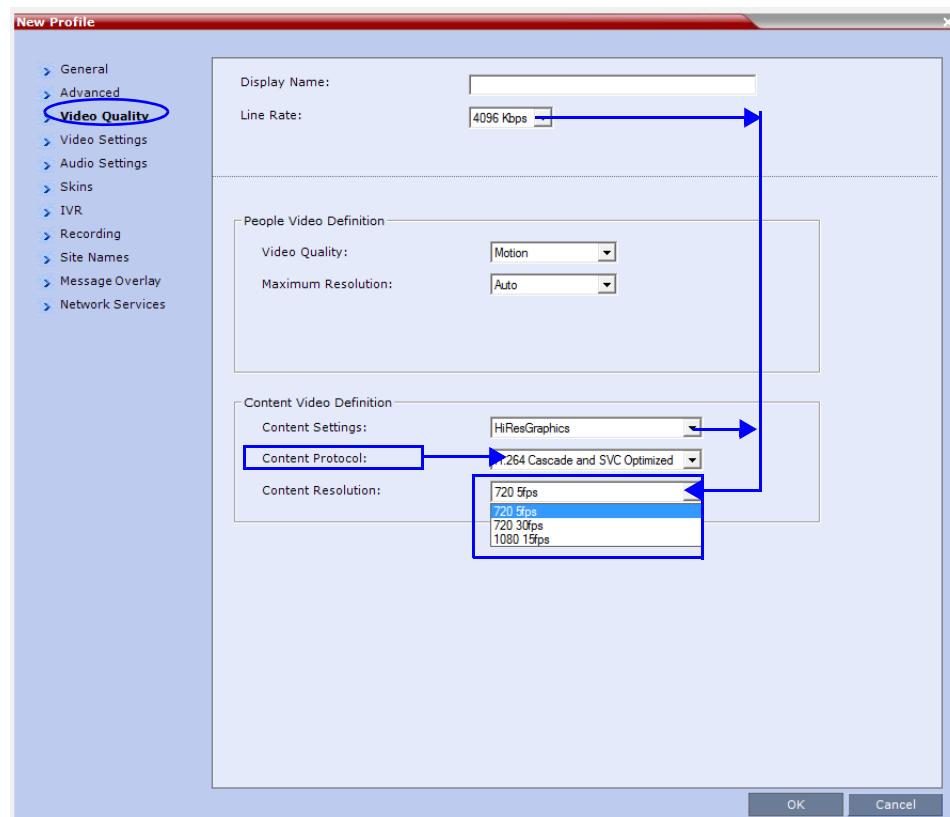
The following table summarizes the interaction of these parameters.

Table 4-8 Bit Rate Allocation to Content Channel by Line Rate, Content Settings & Content Resolution in AVC CP Conferencing

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096
Graphics	HD720/5		64	128	128	256	256	256	512	512
	HD720/30							512	512	512
	HD1080/15						768	768	1152	1152

Table 4-8 Bit Rate Allocation to Content Channel by Line Rate, Content Settings & Content Resolution in AVC CP Conferencing (Continued)

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096
Hi Resolution Graphics	HD720/5			192	256	384	384	512	768	512
	HD720/30							512	768	768
	HD1080/15								768	1152
Live Video	HD720/5			256	384	512	768	768	768	768
	HD720/30					512	768	768	768	768
	HD1080/15						768	768	1152	1152

The selection of the appropriate *Content Resolution* option, when several options are available, should be based on the line rate and capabilities that can be used by most or all endpoints connecting to the conference.

Examples:

* If the conference *Line Rate* is **1024** kbps.

  and

* If the *Content Settings* selection is **Graphics**.

  — **Content Resolutions** of **HD720/5** and **HD1080/15** are selectable with **256** kbps and **768** kbps allocated as the *Conference Content Rate* respectively.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Graphics	HD720/5		64	128	128	256	256	256	512	512
	HD720/30							512	512	512
	HD1080/15						768	768	1152	1152

The higher*Content Resolution,* **HD1080/15** should be selected only if most of the endpoints connecting to the conference can support a *Content Rate* of 768Kbps, which requires the participant to connect to the conference at a *Line Rate* of 1024kbps.

When the lower *Content Resolution* **HD720/5** is selected, the conference *Content Rate* is set to 256 kbps. This will enable the endpoints that connect to the conference at a *Line Rate* of at least 768 kbps to receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 768Kbps, will not receive content.

- If the *Content Settings* selection is **Hi Resolution Graphics**.
  — Only **HD720/5** can be selected as the *Content Resolution* with **384** kbps allocated as the conference *Content Rate*.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Hi Resolution Graphics	HD720/5			192	256	384	384	512	768	512
	HD720/30							512	768	768
	HD1080/15								768	1152

Only endpoints that connect at a *Line Rate* of 768 kbps that is required to support a *Content Rate* of 384 kbps will receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 768 kbps, will not receive content.

- If the *Content Settings* selection is **Live Video**.
  — **HD720/5**, **HD720/30** or **HD1080/15** can be selected as the *Content Resolution* with **768** kbps allocated the as the *Conference Content Rate*.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Live Video	HD720/5			256	384	512	768	768	768	768
	HD720/30					512	768	768	768	768
	HD1080/15						768	768	1152	1152

The higher *Content Resolution* should be selected according to the resolution capabilities of the majority of the endpoints connecting to the conference. Endpoints that cannot support the selected *Content Resolution* are considered *Legacy Endpoints* and will not receive content.

Selecting a Customized Content Rate

Customized Content Rate functionality can be implemented when a *Conference Content Rate*, that is automatically calculated by the Collaboration Server, may not be suitable in a *Cascaded Environment*, where conference line rates may vary widely between the cascaded conferences. For example, one conference may have a line rate of 2 Mbps, and the other a line rate of is 512kbps.

Guidelines:

- Cascaded conferences may have different *Conference Line Rates*.
- The *Customized Content Rate* must be the same for all cascaded conferences.

To Select the Customized Content Rate:

Customized Content Rate is enabled in the *Profile - Video Quality* dialog box.
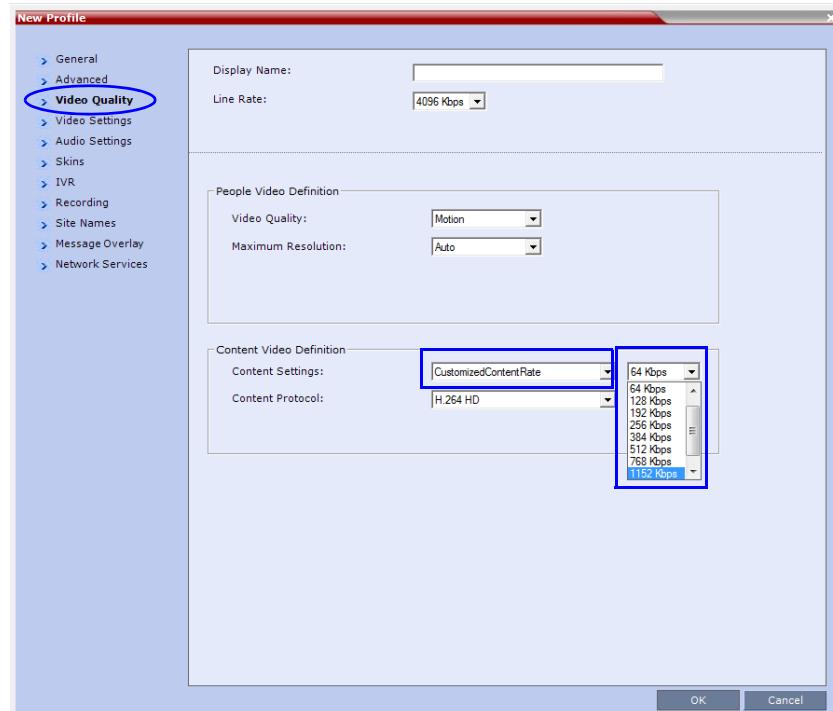
1   In the *Content Settings* list, select **Customized Content Rate**.
    When selected, a drop-down menu of the available *Conference Content Rates* is
    displayed. These *Content Line Rates* are based on and will vary according to the selected
    Conference Line Rate.

    The largest selectable *Content Line Rate* is 66% of the *Conference Line Rate*.

    If the *Conference Line Rate* is 64kbps or 96kbps, the only available *Conference Content Rate*
    is **0**, indicating that *Content* is not supported at these rates.

2   Select the required content rate.

    When selecting a *Conference Line Rate* (after selecting *Customized Content Rate)* that is too
    low for the selected *Customized Content Rate*, the following error message is displayed:
    *"The selected Conference Line Rate is too low to support the selected Content Line Rate. Click
    Cancel and reconfigure either of the Line Rates or click OK to return to the default Content
    Setting."*

    You can then modify either the *Content Line Rate* or the *Conference Line Rate* or select
    another *Content Setting* option.

3 If **H.264 Cascade and SVC Optimized** is the selected *Content Protocol*, a **Content Resolution** must be selected.
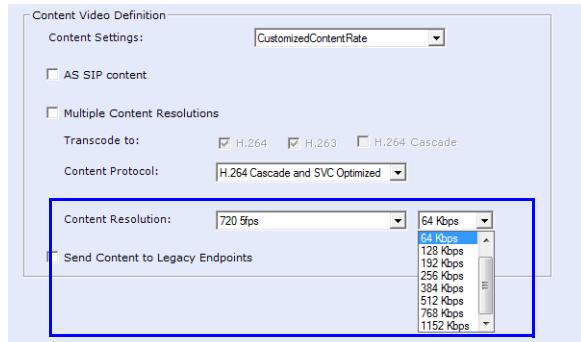
Table 4-9 lists the *Cascade Resolutions* available for the various *Conference Content Rates*.

Table 4-9   *H.264 Cascade and SVC Optimized - Cascade Resolutions*

H.264 Cascade Optimized			
Conference Content Rate (Kbps)	**Available Resolutions**[*]		
64	HD720p5 Content Not Supported		
128	HD720p5		
192	HD720p5		
256	HD720p5		
384	HD720p5		
512	HD720p5	HD720p30	
768	HD720p5	HD720p30	HD1080p15
1152	HD720p5	HD720p30	HD1080p15
1536	HD720p5	HD720p30	HD1080p15

[*]The default resolution for all *Content Rates* is *HD720p5*.

Modifying the Threshold Line Rate for HD Resolution Content

The threshold line rate for *HD Resolution Content* is the line rate at which the Collaboration Server will send *Content* at *HD1080 Resolution*. The default is 768 kbps. When the threshold value is set to 0, HD720p/ HD1080p resolutions for Content sharing are disabled.

To modify the HD Resolution Content threshold line rate:

1 On the Collaboration Server menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2 In the *MCMS_PARAMETERS* tab, double-click the **MIN_H239_HD1080_RATE** entry.
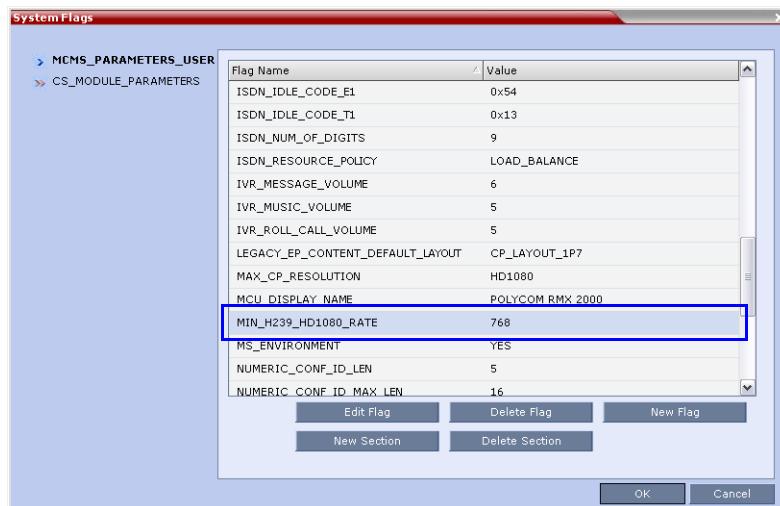
The *Update Flag* dialog box is displayed.

3 In the *Value* field, enter the minimum line rate at which *HD1080 Resolution Content* will be enabled.

— Enter **0** to disable this flag and prevent HD Content from being used.

4 Click **OK** to confirm and exit the *Update Flag* dialog box.

5 Click **Close** to exit the *System Flags* dialog box.

Exclusive Content Mode

Exclusive Content Mode allows you to limit *Content* broadcasting to one participant, preventing other participants from interrupting the *Content* broadcasting while it is active.

Guidelines

- The *Exclusive Content Mode* is enabled or disabled by a check box in the in the *Advanced* tabs of the *Conference Profile*. The check box is cleared (feature is disabled) by default.
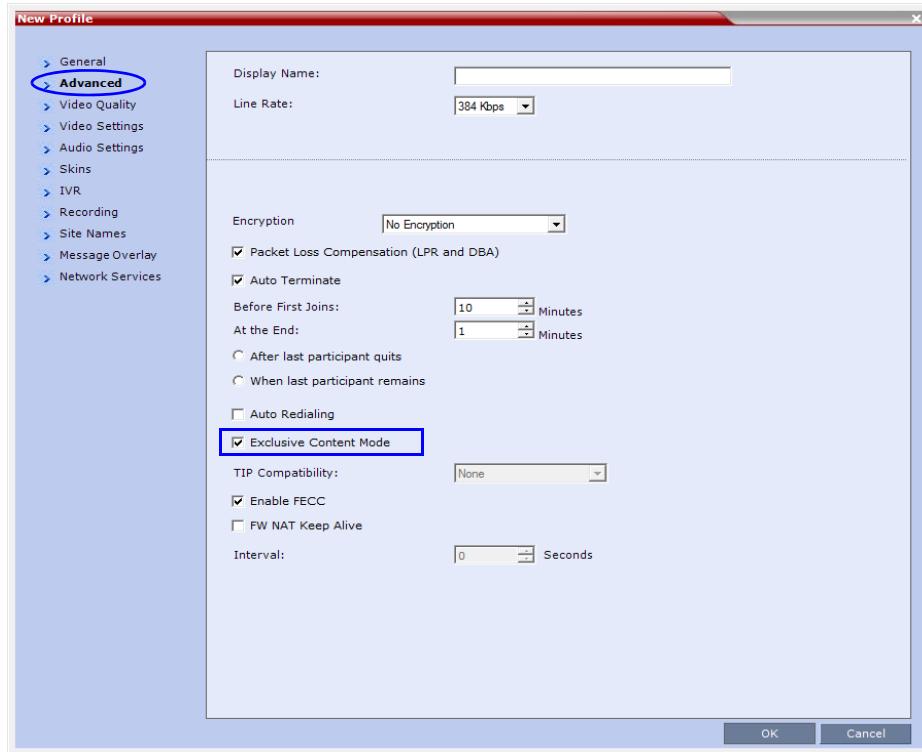
- *Exclusive Content Mode* can be enabled or disabled during an ongoing conference using the *Conference Properties - Advanced* dialog box.
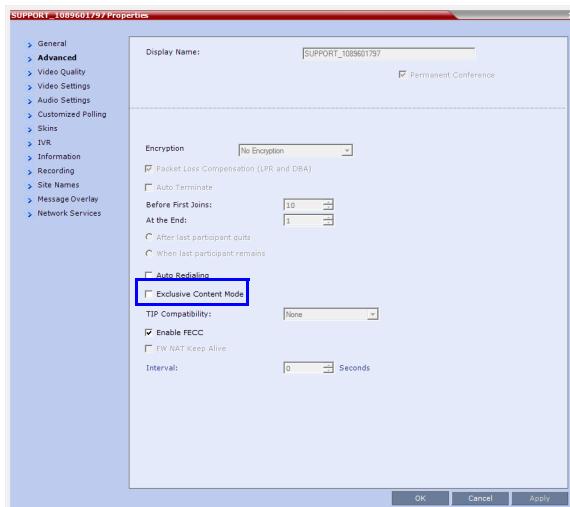
- In *Exclusive Content Mode,* if the RESTRICT_CONTENT_BROADCAST _ TO_LECTURER *System Flag* is set to:

— **NO** - the first participant to send content becomes the *Content Token* holder and has to release the *Content Token* before any other participant can acquire the token and begin transmitting *Content*.

— **YES** - only the designated *Lecturer* can be the *Content Token* holder.

• In *Exclusive Content Mode*, if an endpoint attempts to send *Content* a few seconds after another endpoint sent *Content*, the *Content* stream it is receiving is momentarily interrupted by a slide which is displayed for a few seconds before the normal *Content* stream is resumed.

Stopping a Content Session

In some cases, when one participant ends the Content session from his/her endpoint, the Content token is not released and other participants cannot send Content.

The Collaboration Server User can withdraw the Content token from the current holder and to return it to the MCU for assignment to other endpoints.

To end the current Content session:

>> In the *Conferences* list pane, right-click the conference icon and then click **Abort H.239 Session**.
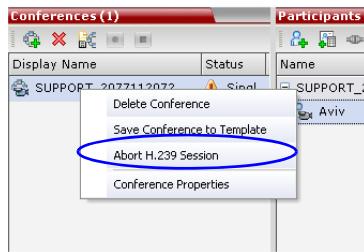
Content Broadcast Control

Content Broadcast Control prevents the accidental interruption or termination of *H.239 Content* that is being shared in a conference.

Content Broadcast Control achieves this by giving *Content Token* ownership to a specific endpoint via the *Collaboration Server Web Client*. Other endpoints are not able to send content until *Content Token* ownership has been transferred to another endpoint via the *Collaboration Server Web Client*.

Guidelines

• *Content Broadcast Control* is supported in *CP* conferences.

• *Content Broadcast Control* is supported in H.323 environments.

• Only the selected *Content Token* owner may send content and *Content Token* requests from other endpoints are rejected.

• *Content Token* ownership is valid until:

— It is canceled by the Collaboration Server User via the *Collaboration Server Web Client*.

— The owner releases it.

— The endpoint of the *Content Token* owner disconnects from the conference.

• The Collaboration Server User can cancel *Content Token* ownership.

- In cascaded conferences, a participant functioning as the cascade link cannot be given token ownership.

Giving and Cancelling Token Ownership

To give token ownership:

1 In the Participants list, right click the AVC-enabled endpoint that is to receive Content Token ownership.
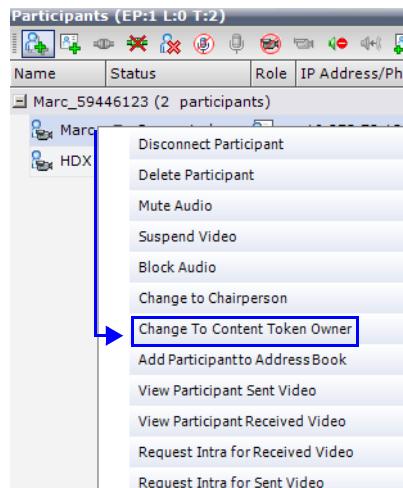
2 Select **Change To Content Token Owner** in the drop-down menu.

The endpoint receives ownership of the *Content Token* and an indication icon is displayed in the Role column of the participant's entry in the Participants list.
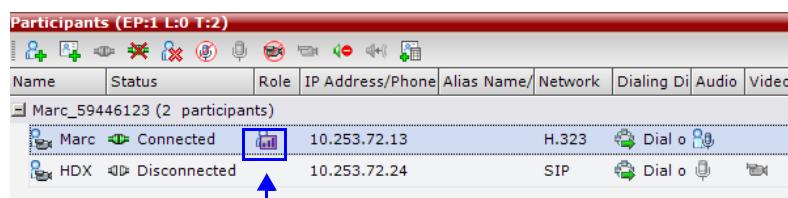
To cancel token ownership:

1   In the *Participants* list, right click the endpoint that currently has *Content Token* ownership.
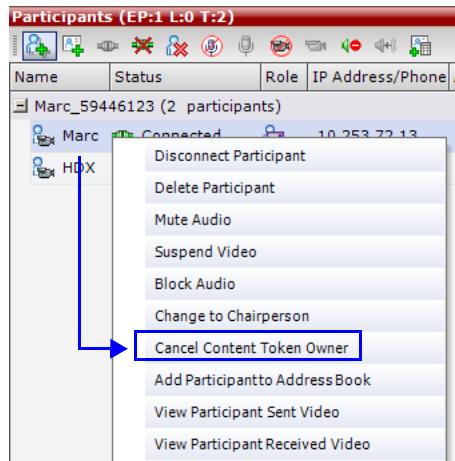
2   Select **Cancel Content Token Owner** in the drop-down menu.
Content Token ownership is cancelled for the endpoint.

Managing Noisy Content Connections

The system can identify participants who send frequent requests to refresh their Content display usually as a result of a problematic network connection. The frequent refresh requests cause frequent refresh of the Content display and degrade the viewing quality.

When the system identifies the noisy participants, the system will automatically suspend the requests to refresh the sent Content to avoid affecting the quality of the Content viewed by other conference participants. This process is controlled by System flags.

Content Display Flags

*   **MAX_INTRA_REQUESTS_PER_INTERVAL_CONTENT**

    Enter the maximum number of refresh (intra) requests for the Content channel sent by the participant's endpoint in a 10 seconds interval that will be dealt by the Collaboration Server system. When this number is exceeded, the Content sent by this participant will be identified as noisy and his/her requests to refresh the Content display will be suspended.
    Default setting: 3

*   **MAX_INTRA_SUPPRESSION_DURATION_IN_SECONDS_CONTENT**

    Enter the duration in seconds to ignore the participant's requests to refresh the Content display.
    Default setting: 10

*   **CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS**

    This flag controls the requests to refresh (intra) the Content sent from the Collaboration Server system to the Content sender as a result of refresh requests initiated by other conference participants.

Enter the interval in seconds between the Intra requests sent from the Collaboration Server to the endpoint sending the Content to refresh the Content display. Refresh requests that will be received from endpoints within the defined interval will be postponed to the next interval.
Default setting: 5

Forcing Other Content Capabilities

- The **H239_FORCE_CAPABILITIES** *System Flag* in *system.cfg* gives additional control over Content sharing:
  — When the flag is set to **NO (default)**, the Collaboration Server only verifies that the endpoint supports the content protocols: *H.263* or *H.264*.
  — When set to **YES**, the Collaboration Server checks frame rate, bit rate, resolution, annexes and all other parameters of the Content mode as declared by an endpoint during the capabilities negotiation phase. If the endpoint does not support the Content capabilities of the MCU, the participant will not be able to send or receive content over a dedicated content channel.

Content Sharing via the Polycom CCS Plug-in for Microsoft Lync Clients

From version 8.1, Polycom CCS (Content Collaboration Solution) Plug-in for Lync clients allows Lync clients to receive and send *Content* on a separate channel, without having to use the video channel. *Content* is transmitted using SIP BFCP.

For more information, see Appendix 4, "*Exclusive Content Mode*"on page **4-16**.

Video Preview

Collaboration Server users can preview the video sent from the participant to the conference (MCU) and the video sent from the conference to the participant. It enables the Collaboration Server users to monitor the quality of the video sent and received by the participant and identify possible quality degradation.

The video preview is displayed in a separate window independent to the *Collaboration Server Web Client*. All Web Client functionality is enabled and conference and participant monitoring as well as all other user actions can be performed while the video preview window is open and active. Live video is shown in the preview window as long as the window is open. The preview window closes automatically when the conference ends or when participant disconnects from the conference. It can also be closed manually by the Collaboration Server user.

Video Preview Guidelines

- Video preview window size and resolution are adjusted to the resolution of the PC that displays the preview.
- Video Preview of the video sent from the conference to the participant is shown according to the line rate and video parameters of the level threshold to which the participant is connected.
- Only one preview window can be displayed for each *Collaboration Server Web Client* connection (workstation).

- Only one preview window can be displayed for a single conference and up to four preview windows can be displayed for each on different workstations (one per workstation and one per conference).
- Live video that is shown in the preview window does not include the Content when it is sent by the participant.
- Video Preview is supported in cascaded conferences.
- If the video preview window is opened when the IVR slide is displayed to the participant, it will also be displayed in the video preview window.
- Video Preview is supported with *H.264 High Profile.*
- Video Preview is disabled in encrypted conferences.
- Video preview cannot be displayed when the participant's video is suspended.
- Participant's video preview and the CMAD window cannot be open and running simultaneously on the same PC as both require the same DirectDraw resource.

Workstation Requirements

To be able to display the video preview window, the following minimum requirements must be met:

- Windows XP, Windows Vista and Windows 7
- Internet Explorer 7 and later
- DirectX is installed
- DirectDraw Acceleration must be enabled and no other application is using the video resource
- Hardware acceleration must be enabled

Testing your Workstation

To ensure that your workstation can display the video preview window:

1 In Windows, click **Start > Run**.
The *Run* dialog box opens.

2 In the *Open* field, type **dxdiag** and press the **Enter** key or click **OK**.
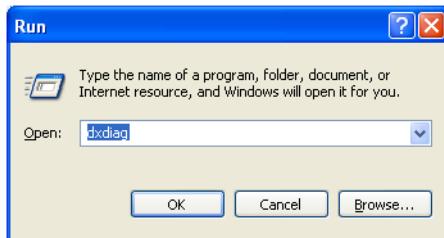
A confirmation message is displayed.

3 Click **Yes** to run the diagnostics.
The *DirectX Diagnostic Tool* dialog box opens.

4 Click the **Display** tab.

To be able to display the video preview window, the **DirectDraw Acceleration** and **Direct3D Acceleration** options must be **Enabled**.
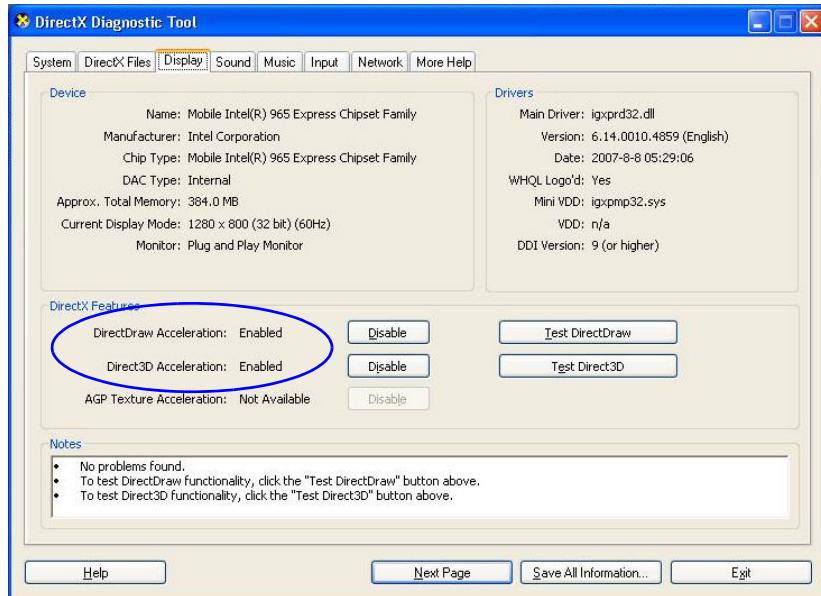
If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed in the Video Preview window.

5 Click the **Exit** button.

Previewing the Participant Video

To preview the participant video:

1 List the conference participants in the *Participants* pane.

2 Right-click the participant whose video you want to preview and then click one of the following options:
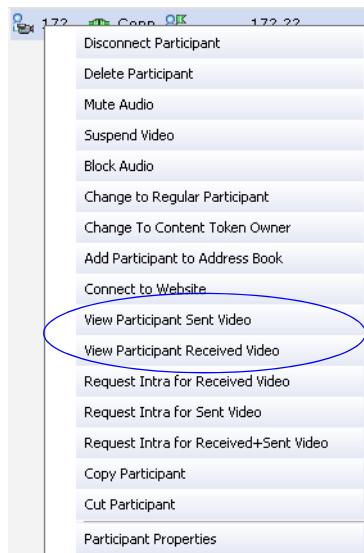
— **View Participant Sent Video** - to display the video sent from the participant to the conference.

— **View Participant Received Video** - to display the video sent from the conference to the participant.

The *Video Preview* window opens.

> If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed.

Auto Scan and Customized Polling in Video Layout

Auto Scan enables a user to define a single cell in the conference layout to cycle the display of participants that are not in the conference layout.

Customized Polling allows the cyclic display to be set to a predefined order for a predefined time period. The cyclic display only occurs when the number of participants is larger than the number of cells in the layout.

Guidelines

- Participants that are in the conference layout will not appear in the *Auto Scan* enabled cell.

- If *Customized Polling* is not used to define the order of the *Auto Scan* it will proceed according to order in which the participants connected to the conference.

- If the user changes the conference layout, the *Auto Scan* settings are not exported to the new layout. If the user changes the conference layout back to the layout in which *Auto Scan* was enabled, *Auto Scan* with the previous settings will be resumed.

Enabling Auto Scan and Customized Polling

Auto Scan

To enable Auto Scan:

1   In the *Collaboration Server Web Client Main Screen - Conference* list pane, double-click the conference or right-click the conference and then click **Conference Properties**.

2   In the *Conference Properties - General* dialog box, click **Video Settings**.
The *Video Settings* tab is displayed.
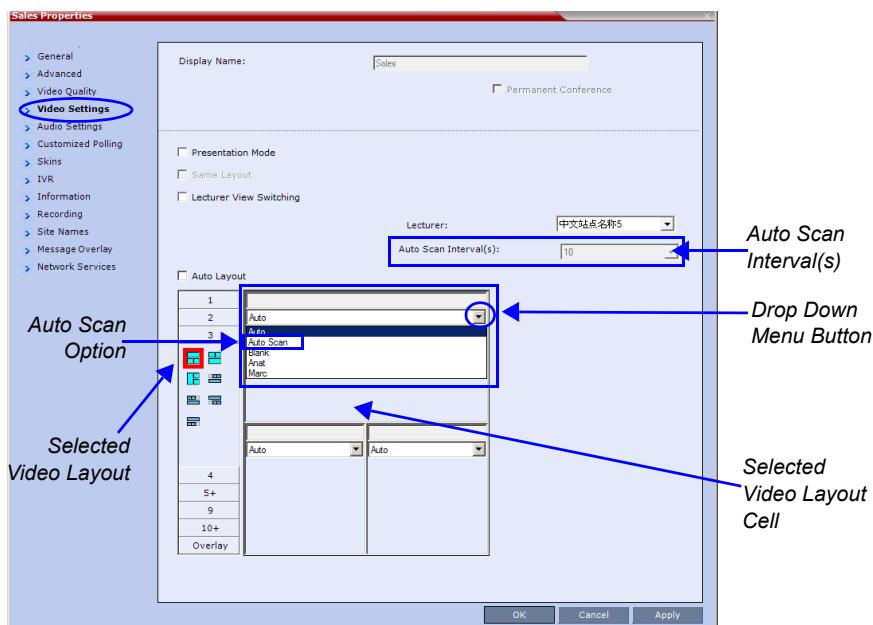
3   If **Auto Layout** check box is selected, clear it.

4   In the video layout cell to be designated for *Auto Scan*, click the drop-down menu button and select **Auto Scan**.

5   Select from the *Auto Scan Interval(s)* drop-down list the scanning interval in seconds.

6   Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open.

-or-

Click **OK** to confirm and close the *Conference Properties* dialog box.

Customized Polling

The order in which the Auto Scanned participants are displayed in the *Auto Scan* enabled cell of the video layout can be customized.

1   Open the *Customized Polling* tab:

a   If the *Video Settings* tab is open click the **Customized Polling** tab.

or

b   In the *Conference* list pane, double-click the conference or right-click the conference and then click **Conference Properties**.

c In the *Conference Properties - General* dialog box, click **Customized Polling**. The *Customized Polling* tab is displayed.
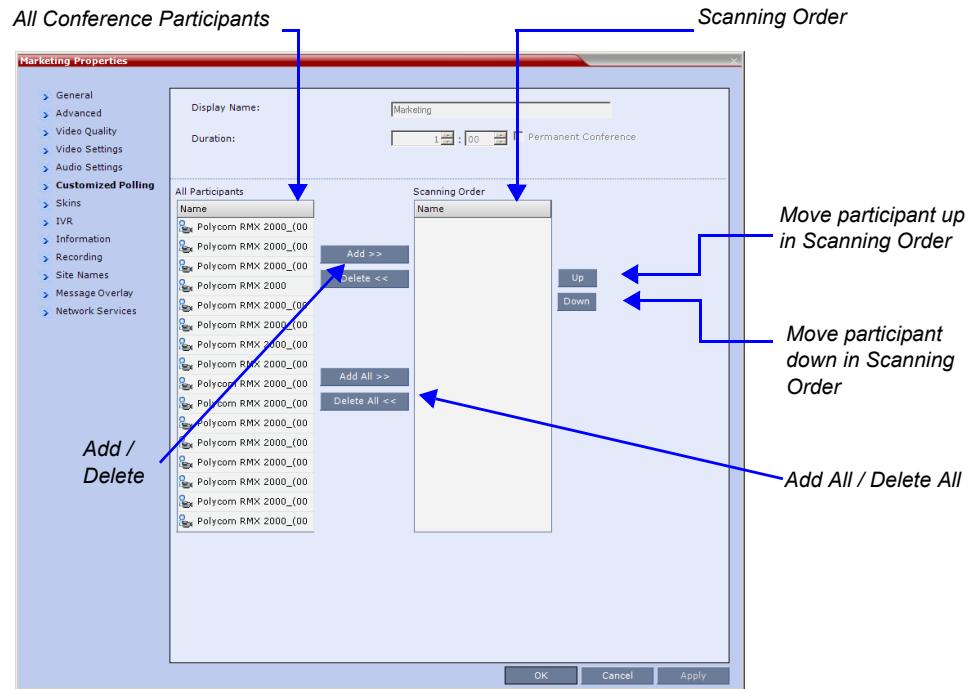
All Conference Participants

Scanning Order

Move participant up in Scanning Order

Move participant down in Scanning Order

Add / Delete

Add All / Delete All

All conference participants are listed in the left pane (*All Participants*) while the participants that are to be displayed in the Auto Scan enabled cell of the video layout are listed in the right pane (*Scanning Order*).

The dialog box buttons are summarized in the following table:

Button	Description
Add	Select a participant and click this button to *Add* a the participant to the list of participants to be Auto Scanned. The participants name is removed from the *All Participants* pane.
Delete	Select a participant and click this button to *Delete* the participant from the list of participants to be *Auto Scanned*. The participants name is moved back to the *All Participants* pane.
Add All	Add all participants to the list of participants to be *Auto Scanned*. All participants' names are removed from the *All Participants* pane.
Delete All	Delete all participant from the list of participants to be *Auto Scanned*. All participants' names are moved back to the *All Participants* pane.
Up	Select a participant and click this button to move the participant *Up* in the *Scanning Order*.
Down	Select a participant and click this button to move the participant *Down* in the *Scanning Order*.

2   **Optional.** Add a participant to the list of participants to be *Auto Scanned*:

— Click on the participant's name in the *All Participants* list and then click the **Add** button to move the participant to the *Scanning Order* pane.

3   **Optional.** Delete a participant from the list of participants to be *Auto Scanned*:

— Click on a participant's name in the *Scanning Order* list and then click the **Delete** button to move the participant back to the *All Participants* pane.

4   **Optional.** Add all participants to the list of participants to be *Auto Scanned* by clicking the **Add All** button.

5   **Optional.** Delete all participant from the list of participants to be *Auto Scanned* by clicking the **Delete All** button.

6   **Optional.** Move the participant up in the *Scanning Order* by clicking the **Up** button.

7   **Optional.** Move the participant down in the *Scanning Order* by clicking the **Down** button.

8   Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open, or click the **OK** the button to confirm and return to the *Collaboration Server Web Client Main Screen*.

Media Encryption

Encryption is available at the conference and participant levels, based on AES 128 (Advanced Encryption Standard) and is fully H.233/H.234 compliant and the Encryption Key exchange DH 1024-bit (Diffie-Hellman) standards.

Media Encryption Guidelines

- Encryption is not available in all countries and it is enabled in the MCU license. Contact Polycom Support to enable it.
- Endpoints must support both AES 128 encryption and DH 1024 key exchange standards which are compliant with H.235 (H.323) to encrypt and to join an encrypted conference.
- The encryption mode of the endpoints is not automatically recognized, therefore the encryption mode must be set for the conference or the participants (when defined).
- Conference level encryption must be set in the Profile, and cannot be changed once the conference is running.
- If an endpoint connected to an encrypted conference stops encrypting its media, it is disconnected from the conference.
- In Cascaded conferences, the link between the cascaded conferences must be encrypted in order to encrypt the conferences.
- The recording link can be encrypted when recording from an encrypted conference to the RSS that is set to encryption. For more information, see *"Recording Link Encryption"* on page **13-7**.
- Encryption of SIP Media is supported using *SRTP* (*Secured Real-time Transport Protocol*) and the *AES* key exchange method.
- Encryption of SIP Media requires the encryption of SIP signaling - TLS Transport Layer must be used.
- Encryption of SIP Media is supported in conferences as follows:

— All media channels are encrypted: video, audio and FECC.

— Collaboration Server SRTP implementation complies with Microsoft SRTP implementation.

— LPR is not supported with SRTP.

— The **ENABLE_SIRENLPR_SIP_ENCRYPTION** *System Flag* enables the *SirenLPR* audio algorithm when using encryption with the *SIP* protocol. The default value of this flag is **NO** meaning *SirenLPR* is disabled by default for *SIP* participants in an encrypted conference. To enable *SirenLPR* the *System Flag* must be added to *system.cfg* and its value set to **YES**.

— The **SEND_SRTP_MKI** *System Flag* enables or disables the inclusion of the *MKI* field in *SRTP* packets sent by the Collaboration Server. The default value of the flag is **YES**. Add the flag to *system.cfg* and set its value set to **NO** to disable the inclusion of the *MKI* field in *SRTP* packets sent by the Collaboration Server when using endpoints that cannot decrypt *SRTP*-based audio and video streams if the *MKI* (*Master Key Identifier*) field is included in *SRTP* packets sent by the Collaboration Server. This *System Flag* should not be set to **NO** when *HDX* endpoints, *Microsoft Office Communicator* and *Lync Clients.* For more information, see "*Modifying System Flags*" on page **20-1**.

Mixing Encrypted and Non-encrypted Endpoints in one Conference

Mixing encrypted and non-encrypted endpoints in one conference is possible, based on the Encryption option "Encrypt When Possible" in the *Conference Profile - Advance* dialog box.

The option "*Encrypt When Possible*" enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. Defined participants that cannot connect encrypted are connected non-encrypted, with the exception of dial-out SIP participants.

The same system behavior can be applied to undefined participants, depending on the setting of the System Flag
FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE:

• When set to **NO** and the conference encryption in the Profile is set to "*Encrypt When Possible*", both *Encrypted* and *Non-encrypted undefined participants* can connect to the same conferences, where encryption is the preferred setting.

• When set to **YES** (default), *Undefined participants* must connect encrypted, otherwise they are disconnected.

For *defined participants*, connection to the conference is decided according to the encryption settings in the conference *Profile,* the *Defined Participant's* encryption settings.

For *undefined participants*, connection to the conference is decided according to the encryption settings in the conference *Profile,* the System Flag setting and the connecting endpoint's *Media Encryption* capabilities.

Direct Connection to the Conference

Table 4-10, summarizes the connection status of participants, based on the encryption settings in the conference *Profile,* the *Defined Participant's* encryption settings or the System Flag setting for undefined participants and the connecting endpoint's *Media Encryption* capabilities.

Table 4-10 *Connection of Defined and Undefined H.323, SIPParticipants to the Conference Based on the Encryption Settings*

Conference Encryption Setting	Defined Participant		Undefined Participant	
	Encryption Setting	Connection status	Connection Status *Flag = No	Connection Status *Flag = YES
No Encryption	Auto	Connected, non-encrypted	Connected non-encrypted (Encryption is not declared by the Collaboration Server, therefore the endpoint does not use encryption)	Connected non-encrypted (Encryption is not declared by the Collaboration Server, therefore the endpoint does not use encryption)
	No	Connected, non-encrypted		
	Yes	Connected only if encrypted. Non-encrypted endpoints are disconnected as encryption is forced for the participant.		
Encrypt All	Auto	Connected, encrypted. Non-encrypted endpoints are disconnected	Connect only if encrypted. Non-encrypted endpoints are disconnected	Connect only if encrypted. Non-encrypted endpoints are disconnected
	No	Disconnected (cannot be added to the conference)		
	Yes	Connected, encrypted		
Encrypt When Possible	Auto	*All defined participants **except** dial-out SIP participants:* Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities. *Defined dial-out SIP participant:* Connect only if encrypted. Non-encrypted endpoints are disconnected.	Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities	Connect only if encrypted. Non-encrypted endpoints are disconnected.
	No	Connected, non-encrypted		
	Yes	Connected, encrypted		

* System Flag = FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Connection to the Entry Queue

An undefined participant connecting to an *Entry Queue* inherits the encryption characteristics of the *Entry Queue* as defined in the *Entry Queue's* profile.

Table 4-11 summarizes the connection possibilities for a participant that is to be moved from an *Entry Queue* to a destination conference for each of the conference *Profile* and Entry Queue encryption options.

Table 4-11 *Connection of Undefined Participants to the Entry Queue Based on the Encryption Settings*

Entry Queue Encryption Setting	Undefined Participant Connection to the Entry Queue	
	*Flag = No	*Flag = YES
No Encryption	Connected, non-encrypted (Encryption is not declared by the Collaboration Server, therefore endpoint does not use encryption)	Connected, non-encrypted (Encryption is not declared by the Collaboration Server, therefore endpoint does not use encryption)
Encrypt All	Connected only if encrypted. Non-encrypted endpoints are disconnected	Connected only if encrypted. Non-encrypted endpoints are disconnected
Encrypt When Possible	Connected encrypted - Endpoints with encryption capabilities. Connected non-encrypted - endpoints without encryption capabilities	Connected only if encrypted. Non-encrypted endpoints are disconnected.

* System Flag = FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Moving from the Entry Queue to Conferences or Between Conferences

When moving participants from the Entry Queue to the destination conference, or when the Collaboration Server user moves AVC participants from one conference to another, the connection rules are similar and they are summarized in Table 4-12:

Table 4-12 *Moving Participants from the Entry Queue to the Destination conference or between conferences Based on the Encryption Settings*

Destination Conference Encryption Setting	Current Participant Encryption Status			
	Encrypted		Non-Encrypted	
	*Flag = NO	*Flag = YES	*Flag = NO	*Flag = YES
No Encryption	Move succeeds, connected encrypted		Move succeeds, connected non-encrypted	
Encrypt All	Move succeeds, connected encrypted.		Move fails, disconnected.	

Table 4-12 *Moving Participants from the Entry Queue to the Destination conference or between conferences Based on the Encryption Settings (Continued)*

Destination Conference Encryption Setting	Current Participant Encryption Status			
	Encrypted		Non-Encrypted	
	*Flag = NO	*Flag = YES	*Flag = NO	*Flag = YES
Encrypt When Possible	Move succeeds, connected encrypted	Move succeeds, connected encrypted	Move succeeds, connected non-encrypted	Connected only if endpoint was a defined participant in the source conference. Otherwise, move fails.

* System Flag = FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Recording Link Encryption

Recording Links are treated as regular participants, however the ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF *System Flag* must be set to YES if a non-encrypted *Recording Link* is to be allowed to connect to an encrypted conference.

Table 4-13 summarizes the connection possibilities for a *Recording Link* that is to be connected to a conference for each of the conference *profile* and *Entry Queue* encryption options.

Table 4-13 *Connections by Recording Link and Conference Encryption Settings*

Conference Profile Setting	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	
	YES	NO
Encrypt All	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected
No Encryption	Connected non-encrypted	Connected non-encrypted
Encrypt when possible	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.

Encryption Flag Settings

To modify the Encryption flags:

1   Click **Setup>System Configuration**.
   The *System Flags* dialog box opens.

2 Set the
**FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILA
BLE_MODE** flag to **YES** or **NO**.

3 If recording will be used in encrypted conferences, set the
ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF flag to **YES**
or **NO**.

4 Click **OK**.

For more information, see "*Modifying System Flags"* on page **20-1**.

5 Reset the MCU for flag changes to take effect.

Enabling Encryption in the Profile

Encryption for the conference is in the Profile and cannot be changed once the conference is
running.

To enable encryption at the conference level:

>> In the *Conference Profile Properties – Advanced* dialog box, select one of the following
Encryption options:
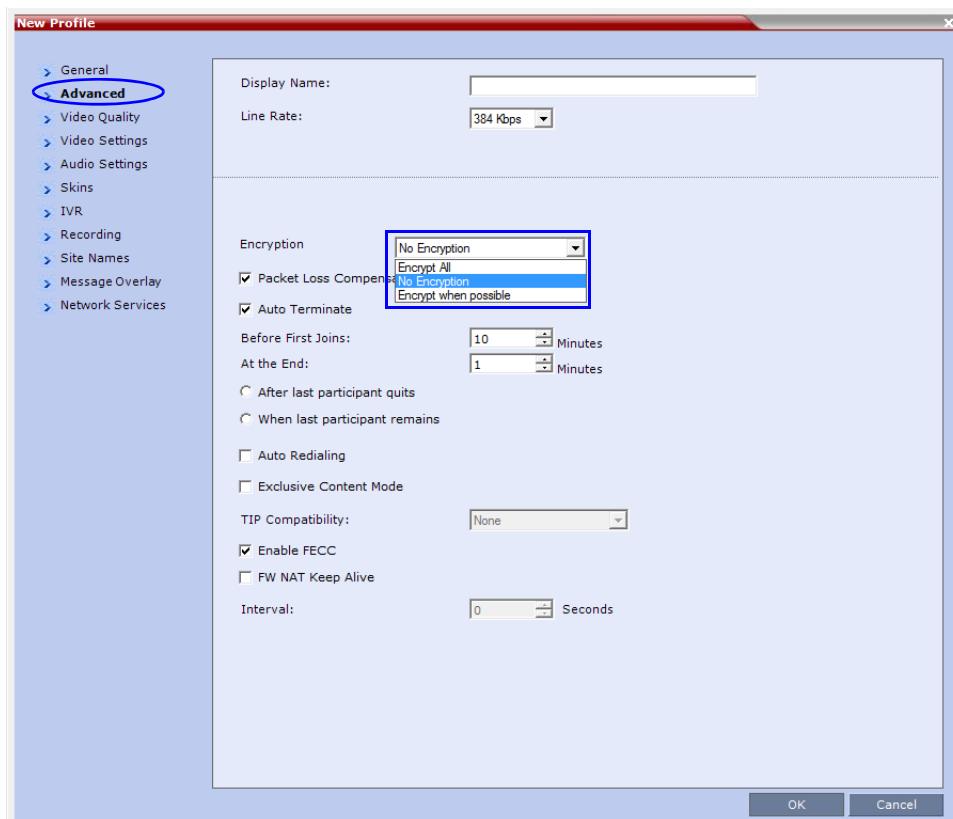
— **Encrypt All** - Encryption is enabled for the conference and all conference
participants must be encrypted.

— **No Encryption** - Encryption is disabled for the conference.

— **Encrypt when possible** - enables the negotiation between the MCU and the
endpoints and let the MCU connect the participants according to their capabilities,

where encryption is the preferred setting. For connection guidelines see "*Mixing Encrypted and Non-encrypted Endpoints in one Conference*" on page **4-28**.

For more information about recording encrypted conferences, see "*Recording Link Encryption*" on page **13-7**.

Enabling Encryption at the Participant Level

You can select the encryption mode for each of the defined participants. Encryption options are affected by the settings of the flag in the system configuration. Undefined participants are connected with the Participant *Encryption* option set to **Auto**, inheriting the conference/ Entry Queue encryption setting.

To enable encryption at the participant level:

>> In the *Participant Properties – Advanced* dialog box, in the *Encryption* list, select one of the following options: **Auto**, **On**, or **Off**.
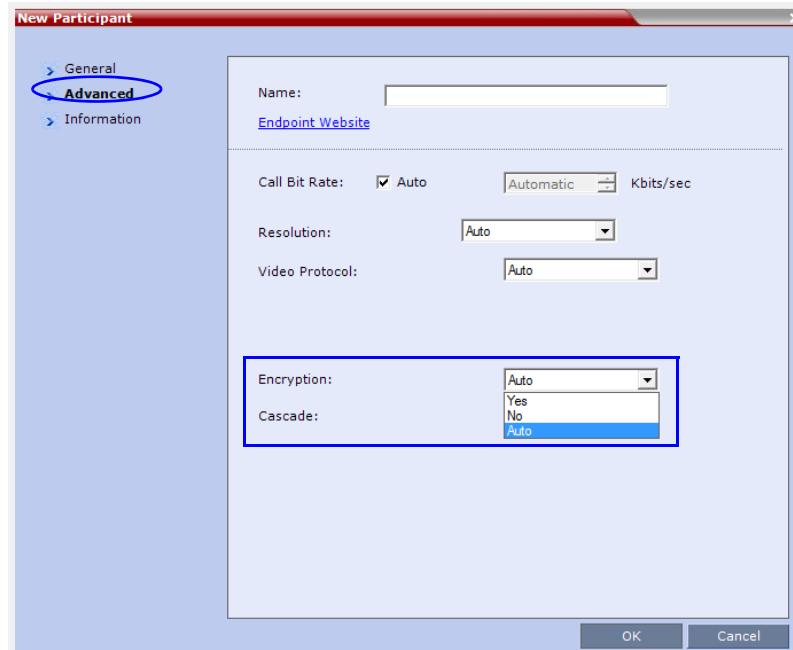
— **Auto** - The participant inherits the conference/Entry Queue encryption setting. The participant connects as encrypted only if the conference is defined as encrypted.

— **Yes** - The participant joins the conference/Entry Queue as *encrypted.*

— **No** - The participant joins the conference/Entry Queue as *non-encrypted*.

Monitoring the Encryption Status

The conference encryption status is indicated in the *Conference Properties - General* dialog box.

The participant encryption status is indicated by a check mark in the *Encryption* column in the *Participants* list pane.

The participant encryption status is also indicated in the *Participant Properties – SDP* tab, where SRTP indication is listed for each encrypted channel (for example, audio and video).
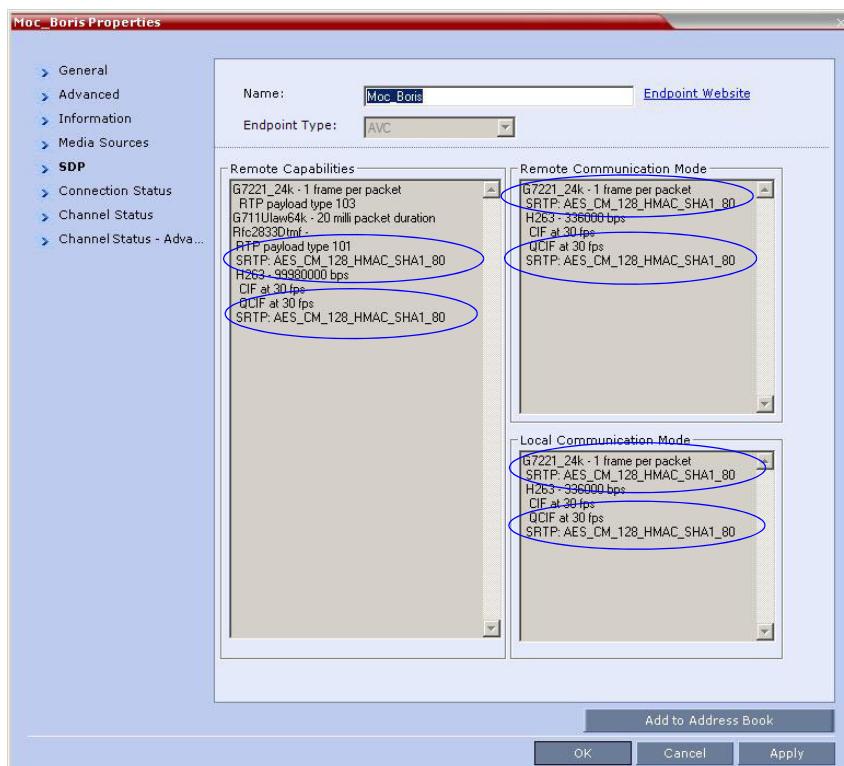
An encrypted participant who is unable to join a conference is disconnected from the conference. The disconnection cause is displayed in the *Participant Properties – Connection Status* tab, *Security Failure* indication, and the *Cause* box identifies the encryption related situation.

For more information about monitoring, see "*Conference and Participant Monitoring*" on page **12-1**.

Packet Loss Compensation (LPR and DBA)

Lost Packet Recovery (*LPR*) and *Dynamic Bandwidth Allocation* (*DBA*) help minimize media quality degradation that can result from packet loss in the network.

Packet Loss

Packet Loss refers to the failure of data packets, transmitted over an IP network, to arrive at their destination. *Packet Loss* is described as a percentage of the total packets transmitted.

Causes of Packet Loss

Network congestion within a LAN or WAN, faulty or incorrectly configured network equipment or faulty cabling are among the many causes of Packet Loss.

Effects of Packet Loss on Conferences

Packet Loss affects the quality of:

*   **Video –** frozen images, decreased frame rate, flickering, tiling, distortion, smearing, loss of lip sync
*   **Audio –** drop-outs, chirping, audio distortion
*   **Content –** frozen images, blurring, distortion, slow screen refresh rate

Lost Packet Recovery

The *Lost Packet Recovery* (*LPR*) algorithm uses *Forward Error Correction* (*FEC*) to create additional packets that contain recovery information. These additional packets are used to reconstruct packets that are lost, for whatever reason, during transmission. *Dynamic Bandwidth Allocation* (*DBA*) is used to allocate the bandwidth needed to transmit the additional packets.

Lost Packet Recovery Guidelines

*   If packet loss is detected in the packet transmissions of either the video or Content streams:
    — *LPR* is applied to both the video and Content streams.
    — *DBA* allocates bandwidth from the video stream for the insertion of additional packets containing recovery information.
*   *LPR* is supported in H.323 and *SIP* networking environments only.
*   In *LPR*-enabled *Continuous Presence* conferences:
    — Both *LPR*-enabled and non-*LPR*-enabled endpoints are supported.
    — The *LPR* process is not applied to packet transmissions from non-*LPR*-enabled H.323 and SIP endpoints.
    — Non-LPR-enabled endpoints can be moved to *LPR*-enabled conferences.
    — LPR-enabled endpoints **cannot** be moved to non-*LPR*-enabled conferences.
*   When connecting via an *Entry Queue:*
    — A participant using an *LPR*-enabled endpoint can be moved to a non-*LPR*-enabled conference. The participant is connected with LPR enabled.

Enabling Lost Packet Recovery

LPR is enabled or disabled in the *Conference Profile* dialog box.

• **CP Conferences** – *LPR* is enabled by default in the *New Profile – Advanced* dialog box. For more information, see "*Defining New Profiles"* on page **2-9**.

Monitoring Lost Packet Recovery

In the *Participant Properties – H.245* tab, *LPR* activity is displayed in all three panes.
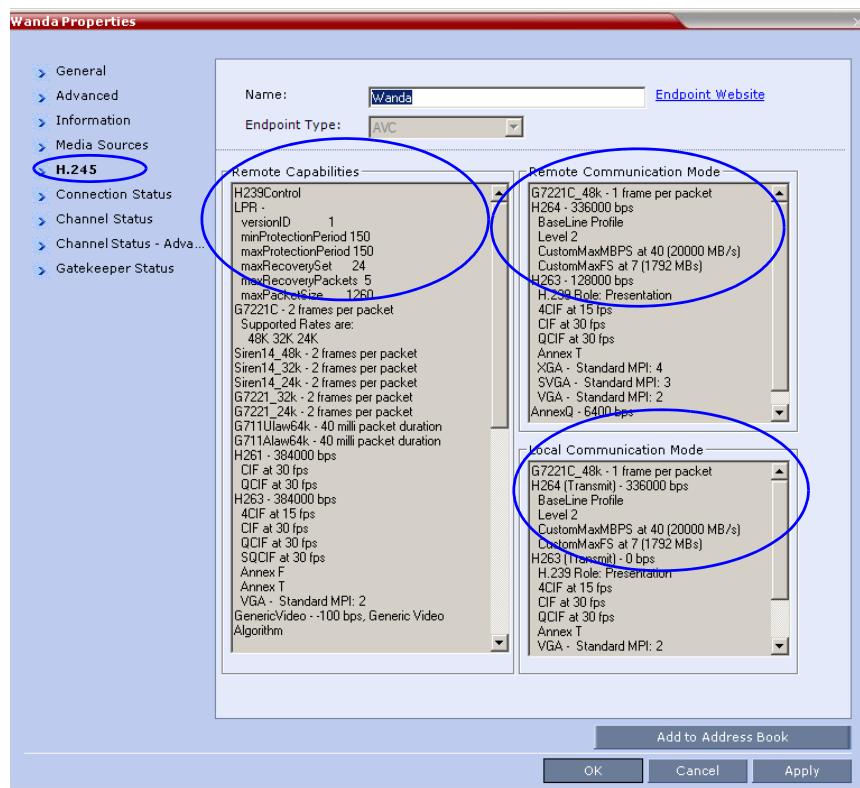
In the *Participant Properties – Channel Status* tab, check box indicators show *LPR* activation in the local and remote (transmit and receive) channels.
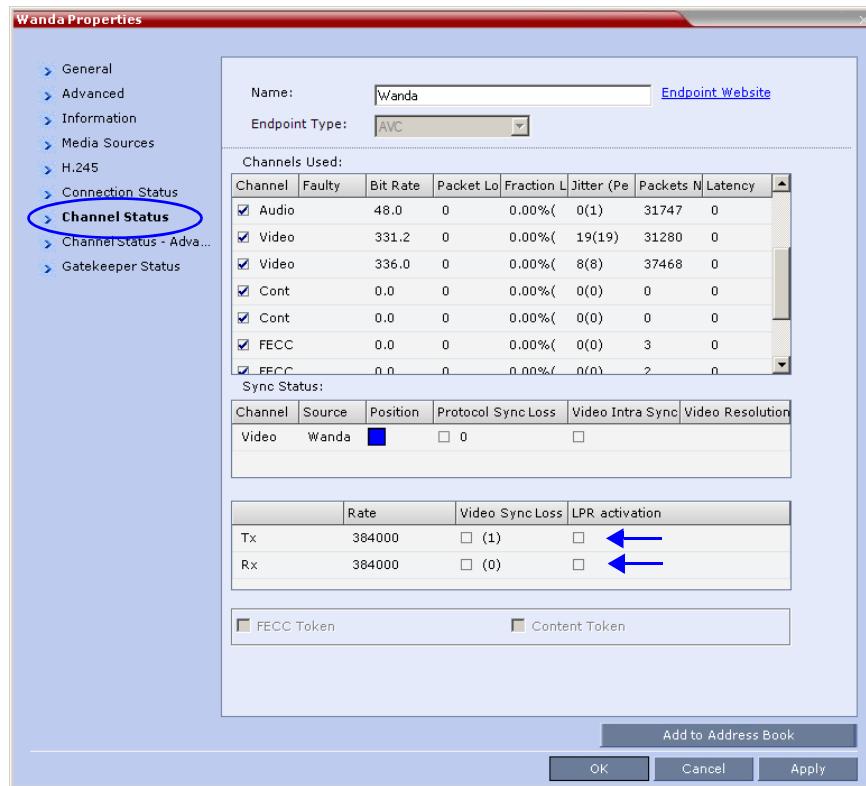
Lecture Mode

Lecture Mode enables all participants to view the lecturer in full screen while the conference lecturer sees all the other conference participants in the selected layout while he/she is speaking. When the number of sites/endpoints exceeds the number of video windows in the layout, switching between participants occurs every 15 seconds. Conference participants cannot change their Personal Layouts while Lecture Mode is enabled.

Automatic switching is suspended when one of the participants begins talking, and it is resumed automatically when the lecturer resumes talking.

Enabling Lecture Mode

Lecture Mode is enabled at the conference level by selecting the lecturer. Conference participants cannot change their Personal Layouts while Lecture Mode is enabled.

Automatic switching between participants viewed on the lecturer's screen is enabled in the conference Profile.

Selecting the Conference Lecturer

Selecting a lecturer for the ongoing conference, enables the Lecture Mode. You can select the lecturer:

- during the definition of the ongoing conference
- after the conference has started and the participants have connected to the conference.

To select the lecturer and enable the Lecture Mode while starting the conference:

>> In the *Conference Properties - Participant* dialog box, enable the Lecture Mode in one of the following methods:
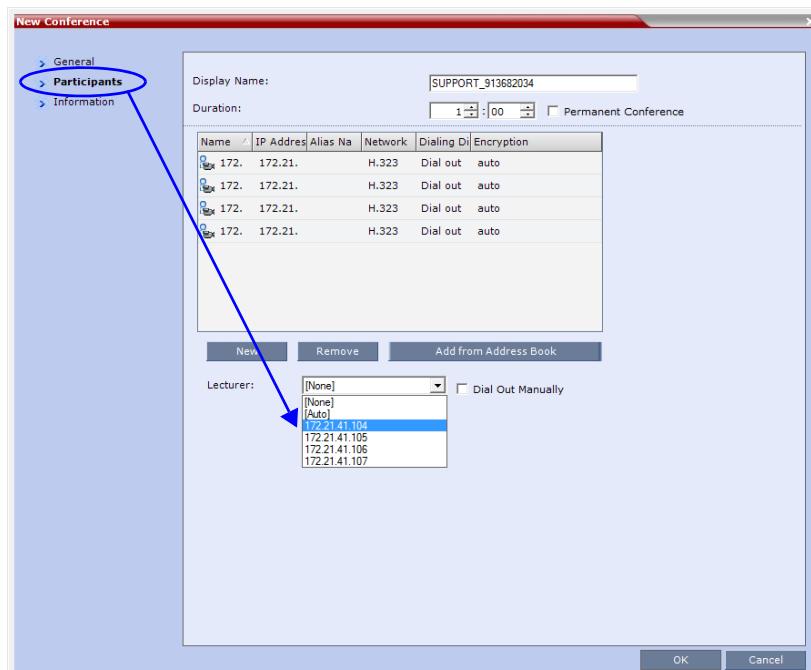
Selecting a defined participant:

a Add participants to the conference either from the Address book or by defining new participants.

b In the **Lecturer** field, select the lecturer from the list of the defined participants.

Automatic selection of the lecturer:

— In the **Lecturer** field, select **[Auto]**.
  In this mode, the conference speaker becomes the lecturer.

To select the lecturer and enable the Lecture Mode during the ongoing conference:

1 Make sure that the participant you want to designate as the lecturer has connected to the conference.

2 In the *Conference Properties - Video Settings* dialog box, in the **Lecturer** field, select the lecturer from the list of the connected participants.
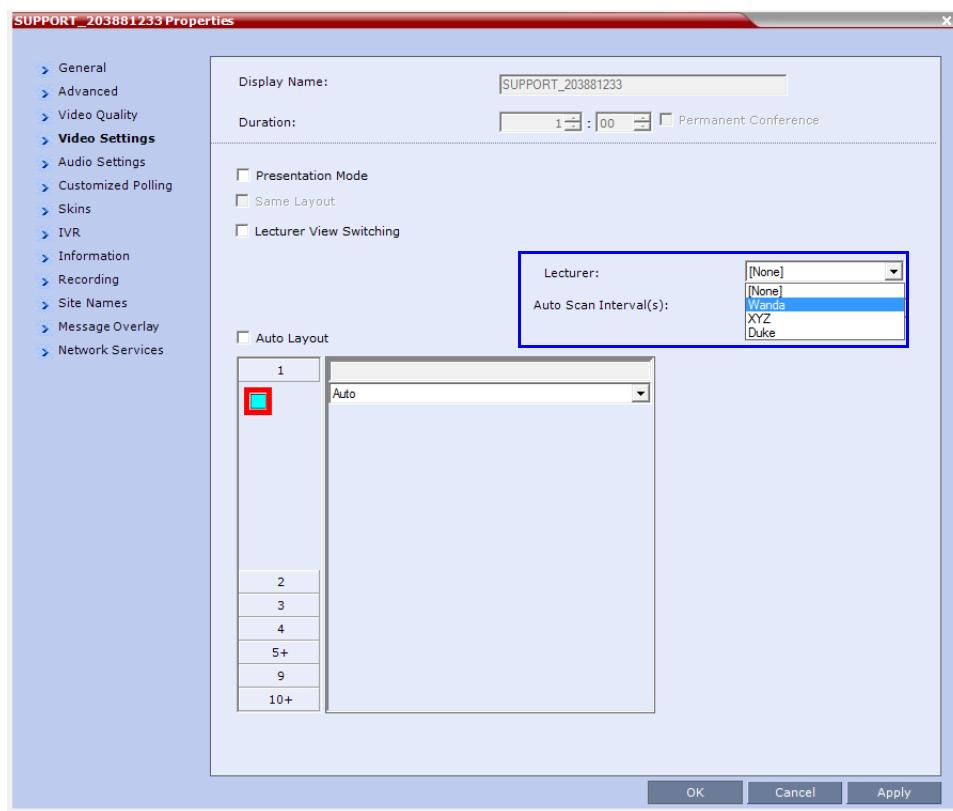
Defined dial out participants and dial in participants are considered to be two separate participants even if they have the same IP address/number. Therefore, if a defined dial-out participant is added to the conference and the same participant then dials in (before the system dialed out to that participant) the system creates a second participant in the Participants list and tries to call the dial-out participant. If the dial-out participant was designated as the conference lecturer, the system will not be able to replace that participant with the dial-in participant that is connected to the conference.

Enabling the Automatic Switching

Automatic switching between participants viewed on the lecturer's screen is enabled in the conference Profile, or during the ongoing conference, in the Conference Properties.

>> In the *Profile Properties - Video Settings* dialog box, select the **Lecturer View Switching** check box.
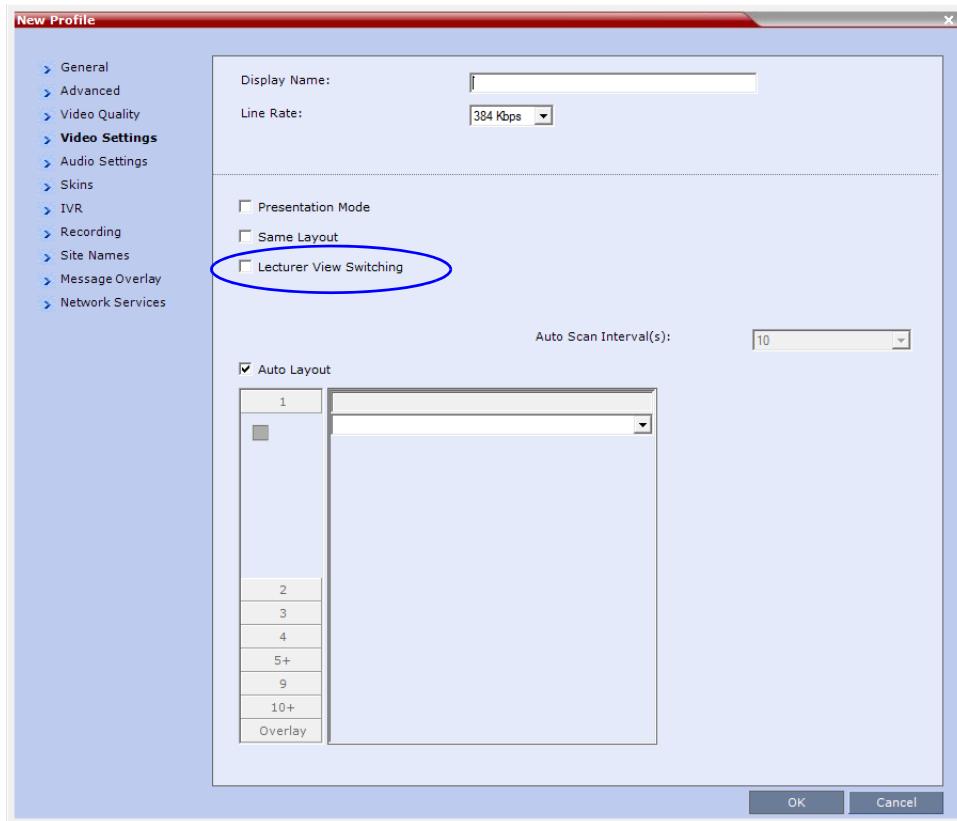
This option is activated when the conference includes more sites than windows in the selected layout. If this option is disabled, the participants will be displayed in the selected video layout without switching.

For more information about Profile definition, see "*Defining AVC - CP Conferencing Profiles*" on page **2-10**.

>> Once the conference is running, in the *Conference Properties - Video Settings* dialog box, select the **Lecturer View Switching** check box.

Lecture Mode Monitoring

A conference in which the Lecture Mode is enabled is started as any other conference. The conference runs as an audio activated Continuous Presence conference until the lecturer connects to the conference. The selected video layout is the one that is activated when the conference starts. Once the lecturer is connected, the conference switches to the Lecture Mode.

When *Lecturer View Switching* is activated, it enables automatic switching between the conference participants in the lecturer's video window. The switching in this mode is not determined by voice activation and is initiated when the number of participants exceeds the number of windows in the selected video layout. In this case, when the switching is performed, the system refreshes the display and replaces the last active speaker with the current speaker.

When one of the participants is talking, the automatic switching is suspended, showing the current speaker, and it is resumed when the lecturer resumes talking.

If the lecturer is disconnected during an Ongoing Conference, the conference resumes standard conferencing.

Forcing is enabled at the Conference level only. It applies only to the video layout viewed by the lecturer as all the other conference participants see only the lecturer in full screen.

If an asymmetrical video layout is selected for the lecturer (i.e. 3+1, 4+1, 8+1), each video window contains a different participant (i.e. one cannot be forced to a large frame and to a small frame simultaneously).

When *Lecture Mode* is enabled for the conference, the lecturer is indicated by an icon (⬛) in the *Role* column of the *Participants* list.

Participant designated as the Lecturer

To control the Lecture Mode during an Ongoing Conference:

During the Ongoing Conference, in the *Conference Properties - Video Settings* dialog box you can:

- Enable or disable the Lecture Mode and designate the conference lecturer in the *Lecturer* list; select **None** to disable the Lecture Mode or select a participant to become the lecturer to enable it.

- Designate a new lecturer.
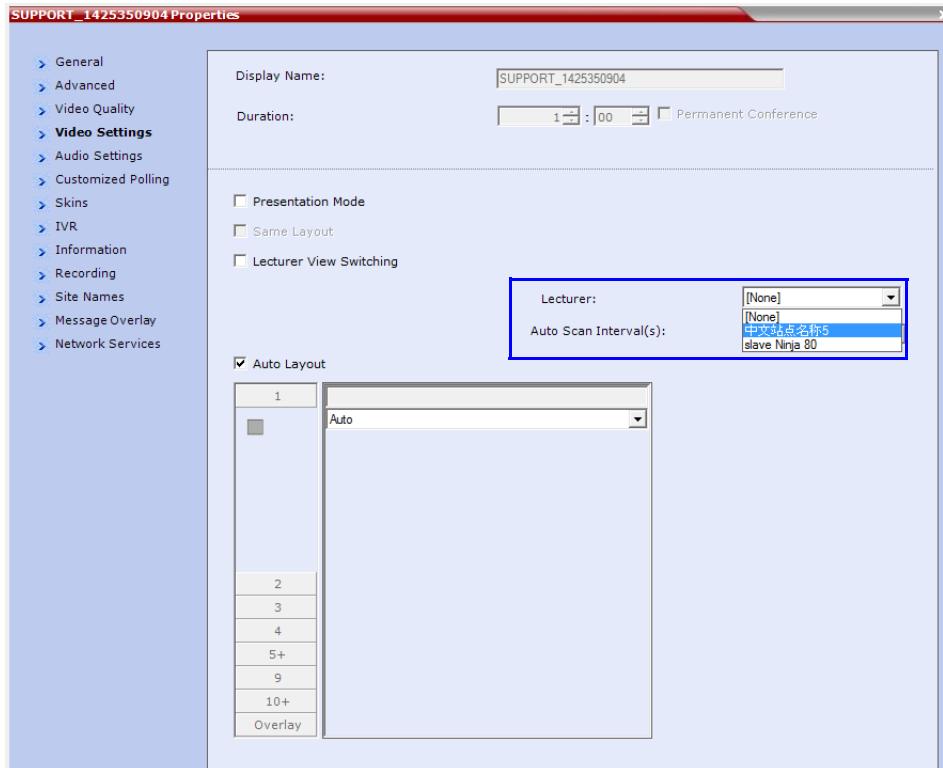
- Enable or disable the *Lecturer View Switching* between participants displayed on the lecturer monitor by selecting or clearing the **Lecturer View Switching** check box.
- Change the video layout for the lecturer by selecting another video layout.

Restricting Content Broadcast to Lecturer

Content broadcasting can be restricted to the conference lecturer only, when one of the conference participants is set as the lecturer (and not automatically selected by the system). Restricting the Content Broadcast prevents the accidental interruption or termination of H.239 Content that is being shared in a conference.

Content Broadcast restriction is enabled by setting the **RESTRICT_CONTENT_BROADCAST_TO_LECTURER** *system flag* to **ON**. When set to OFF (default) it enables all users to send Content.

When enabled, the following rules apply:

- Content can only be sent by the designated lecturer. When any other participant tries to send Content, the request is rejected.
- If the Collaboration Server user changes the designated lecturer (in the *Conference Properties - Video Settings* dialog box), the Content of the current lecturer is stopped immediately and cannot be renewed.
- The Collaboration Server User can abort the H.239 Session of the lecturer.
- Content Broadcasting is not implemented in conferences that do not include a designated lecturer and the lecturer is automatically selected by the system (for example, in *Presentation Mode*).

Muting Participants Except the Lecturer

When the *Mute Participants Except Lecturer* option in the *Conference Profile* is enabled, the audio of all participants in the conference except for the lecturer can be automatically muted upon connection to the conference. This prevents other conference participants from accidentally interrupting the lecture, or from a noisy participant affecting the audio quality of the entire conference. Muted participants cannot unmute themselves unless they are unmuted from the Collaboration Server Web Client/RMX Manager.

Guidelines

- Both administrators and operators (users) are allowed to set the *Mute Participants Except Lecturer* option.

- When the *Mute Participants Except Lecturer* option is enabled, the mute indicator on the participant endpoints are not visible because the mute participants was initiated by the MCU. Therefore, it is recommended to inform the participants that their audio is muted by using the *Message Overlay* functions.

- When the *Mute Participants Except Lecturer* option is enabled in the *Conference Profile* settings, all conferences to which this profile is assigned will start with this option enabled. All participants, except for the designated lecturer, are muted.

- The *Mute Participants Except Lecturer* option can be enabled or disabled at any time after the start of the conference. When enabled, it allows all the conference participants to converse before the lecturer joins the conference or before they are muted. When disabled, it unmutes all the participants in the conference.

- If the endpoint of the designated lecturer is muted when the lecturer connects to the conference, the lecturer remains muted until the endpoint has been unmuted.

- When you replace a lecturer, the MCU automatically mutes the previous lecturer and unmutes the new lecturer.

- When you disconnect a lecturer from the conference or the lecturer leaves the conference, all participants remain muted but are able to view participants in regular video layout until the you disable the *Mute Participants Except Lecturer* option.

- A participant can override the *Mute Participants Except Lecturer* option by activating the *Mute All Except Me* option using the appropriate DTMF code, provided the participant has authorization for this operation in the IVR Services properties. The lecturer audio is muted and the participant audio is unmuted. You can reactivate the *Mute Participants Except Lecturer* option after a participant has previously activated the *Mute All Except Me* option. The participant is muted and the lecturer, if designated, is unmuted.

- In cascaded conferences, all participants (including the link participants) except the lecturer are muted. Only the lecturer is not muted.

Enabling the Mute Participants Except Lecturer Option

The *Mute Participants Except Lecturer* option is enabled or disabled (default) in the *Conference Profile* or in an ongoing conference in the *Profile Properties - Audio Settings* tab.
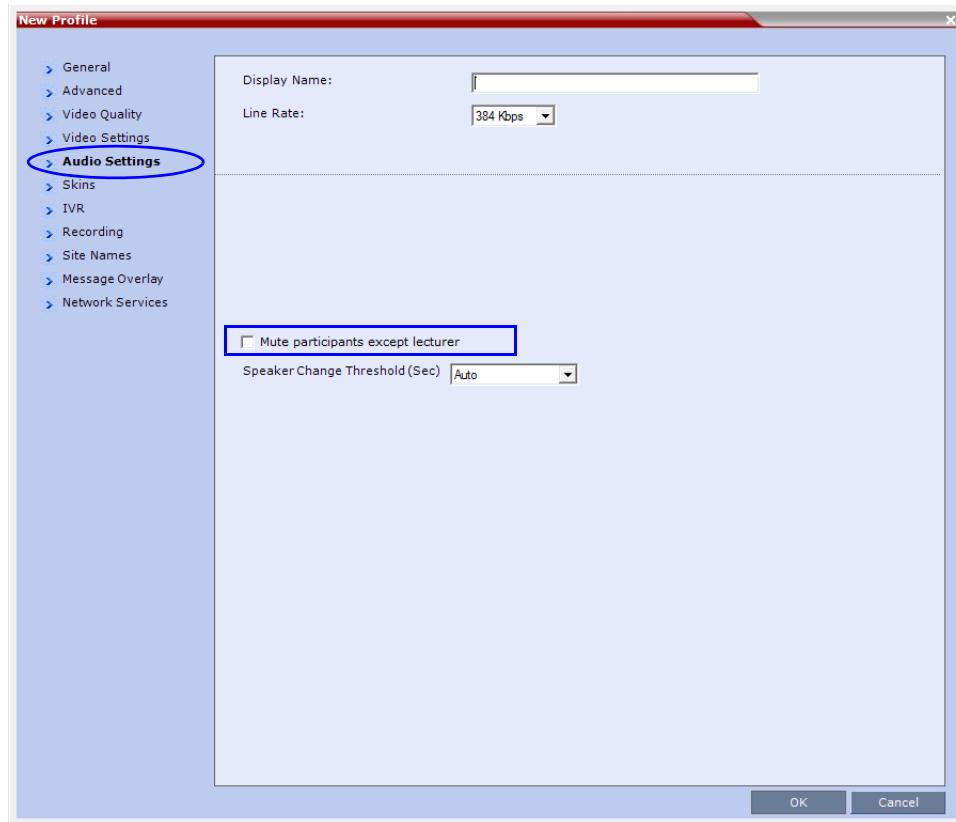
When the *Mute Participants Except Lecturer* option is enabled and a conference has started, the **Mute by MCU** icon is displayed in the *Audio* column in the *Participants* pane of each participant that is muted.

Audio Algorithm Support

The Collaboration Server supports the following audio algorithms: G.711, G.722, G.722.1, G.722.1C, G.729A, Polycom Siren 7 (in mono), Siren14, Siren 22 (in mono or stereo) and SirenLPR.

Polycom's proprietary *Siren 22* is supported for participants connecting with *Polycom* endpoints.

The *Siren 22* audio algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications. *Siren 22* requires less computing power and has much lower latency than alternative wideband audio technologies.

The SirenLPR audio algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications.

Guidelines

- *Siren 22* and *G.719* are supported in both mono and stereo.
- Stereo is supported in *H.323* calls only.
- *Siren 22* is supported by Polycom HDX and Group series endpoints.
- *SirenLPR* is enabled by default and can be disabled by setting the system flag, **ENABLE_SIRENLPR**, to **NO**.
- *SirenLPR* is supported:
  — In IP (H.323, SIP) calls only.
  — With *Polycom CMAD* and *HDX "Canyon"* and Group series endpoints.
  — For mono audio at audio line rates of 32Kbps, 48Kbps and 64Kbps.
  — For stereo audio at audio line rates of 64Kbps, 96Kbps and 128Kbps.

SIP Encryption

The **ENABLE_SIRENLPR_SIP_ENCRYPTION** *System Flag* enables the *SirenLPR* audio algorithm when using encryption with the *SIP* protocol.

The default value of this flag is **NO** meaning *SirenLPR* is disabled by default for *SIP* participants in an encrypted conference. To enable *SirenLPR* the *System Flag* must be added to *system.cfg* and its value set to **YES**.

Mono

The *Siren 22* and *SirenLPR* mono audio algorithms are supported at the following bit rates:

Table 4-14   *Siren22 and SirenLPR Mono vs Bitrate*

Audio Algorithm	Minimum Bitrate (kbps)
Siren22 64k	
Siren22 48K	
Siren22_32k	
Siren22_48K	
G.7221C_48k	
Siren14_48k	

Table 4-14   Siren22 and SirenLPR Mono vs Bitrate (Continued)

Audio Algorithm	Minimum Bitrate (kbps)
SirenLPR_32k	128
Siren22_32k	
G.7221C_32k	
Siren14_32k	
SirenLPR	64
SirenLPR	48
SirenLPR	32

Stereo

The *Siren 22Stereo, G.719Stereo* and *SirenLPR* audio algorithms are supported at the following bit rates.

Table 4-15   Siren22Stereo, G.719Stereo and SirenLPR vs Bitrate

Audio Algorithm	Minimum Bitrate (kbps)
Siren22Stereo_128k	1024
SirenLPRStereo_128k	
Siren22Stereo_96k	512
SirenLPRStereo_96k	
Siren14Stero_96k	
SirenLPRStereo_64k	384
Siren22Stereo_64k	
Siren14Stereo_64k	

Monitoring Participant Audio Properties

The audio algorithm used by the participant's endpoint can be verified in the Participant Properties - Channel Status dialog box.

To view the participant's properties during a conference:

1   In the *Participants* list, right click the desired participant and select **Participant Properties**.

2   Click the **Channel Status - Advanced** tab.
The *Participant Properties - Channel Status - Advanced* dialog box is displayed.

3 In the *Channel Info* field, select **Audio In** or **Audio Out** to display the audio parameters.
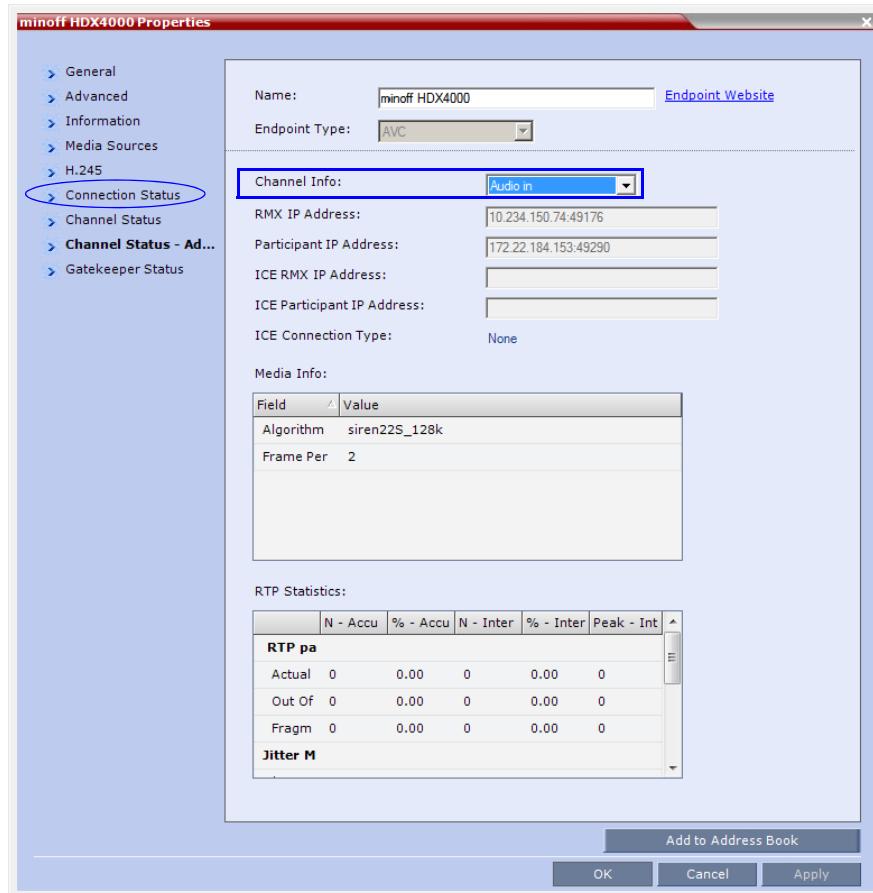
4 Click the **OK** button.

Permanent Conference

A *Permanent Conference* is any ongoing conference with no pre-determined *End Time* continuing until it is terminated by an administrator, operator or chairperson.

Guidelines

- Resources are reserved for a *Permanent Conference* only when the conference has become ongoing.
- Resources are allocated to a *Permanent Conference* according to the *Reserve Resources for Video Participants* field. If the number of defined dial-out participants exceeds the value of this field, the Collaboration Server automatically replaces the number in the *Reserve Resources for Video Participants* field with the number of defined dial-out participants in the *Permanent Conference.*
- *Auto Terminate* is disabled in *Permanent Conferences*.
- If participants disconnect from the *Permanent Conference*, resources that were reserved for its video and audio participants are released.
- *Entry Queues*, *Conference Reservations* and *SIP Factories* cannot be defined as *Permanent Conferences*.
- Additional participants can connect to the conference, or be added by the operator, if sufficient resources are available.
- The maximum size of the *Call Detail Record* (*CDR*) for a *Permanent Conference* is 1MB.

Enabling a Permanent Conference

The *Permanent Conference* option is selected in the *New Conference, New Meeting Room* or *New Conference Templates* dialog boxes.

New Conference   New Meeting Room   New Conference Template

5
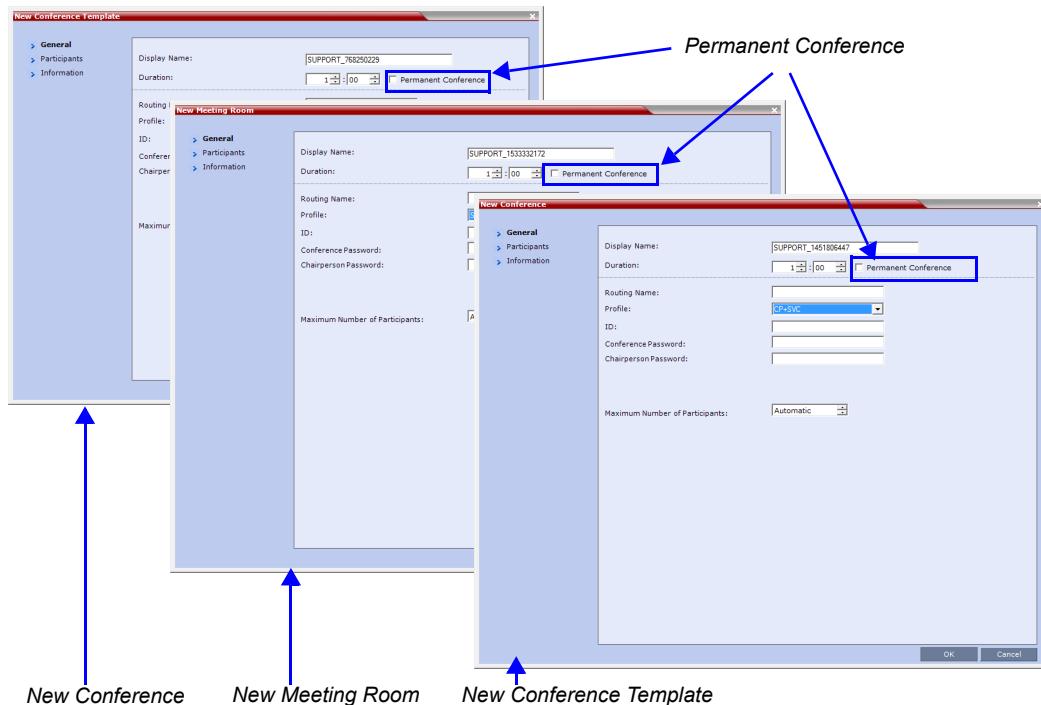
Cascading Conferences

Cascading enables administrators to connect one conference directly to one or several conferences, depending on the topology, creating one large conference. The conferences can run on the same MCU or different MCUs.

There are many reasons for cascading conferences, the most common are:

- Connecting two conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, for example, different communication protocols, such as, serial connections and ISDN, etc....

The following cascading topologies are available for cascading:

- **Basic Cascading** - only two conferences are connected (usually running on two different Collaboration Servers). The cascaded MCUs reside on the same network.
- **Star Cascading** - one or several conferences are connected to one master conference. Conferences are usually running on separate MCUs. The cascaded MCUs reside on the same network.
- **MIH (Multi-Hierarchy) Cascading** - several conferences are connected to each other in Master-Slave relationship. The cascaded MCUs can reside on different networks.

System configuration and feature availability change according to the selected cascading topology.

Video Layout in Cascading conferences

Cascade links are treated as endpoints in CP conferences and are allocated resources according to *"Default Minimum Threshold Line Rates and Resource Usage Summary"* on page **3-9**. Cascaded links in 1x1 video layout are in SD resolution.

When cascading two conferences, the video layout displayed in the cascaded conference is determined by the selected layout in each of the two conferences. Each of the two conferences will inherit the video layout of the other conference in one of their windows.

In order to avoid cluttering in the cascaded window, it is advised to select appropriate video layouts in each conference before cascading them.

<table>
<tr><td>During Cascading</td><td></td><td></td></tr>
</table>

Video layout of Conf. B in window of Conf. A

Video layout of Conf. A in window of Conf. B

Figure 5-1 *Video Layouts in Cascaded Conferences*

Guidelines

To ensure that conferences can be cascaded and video can be viewed in all conferences the following guidelines are recommended:

- The same version installed on all MCUs participating the cascading topology
- The same license installed on all MCUs participating the cascading topology
- Same Conference Parameters are defined in the Profile of the conferences participating in the cascading topology
  — Conference line rates should be identical
  — Content rate should be identical
  — Same encryption settings
- DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences
- DTMF forwarding is suppressed
- The video layout of the link is set to 1x1 by the appropriate system flag.
- When the Mute Participants Except Lecturer option is enabled in the Conference Profile, all participants (including the link participants) except the lecturer are muted. Only the lecturer is not muted.
- *Gathering* is not supported in *Cascading Conferences*.

Flags Controlling Cascade Layouts

- Setting the **FORCE_1X1_LAYOUT_ON_CASCADED_LINK _CONNECTION** *System Flag* to **YES** (default) automatically forces the cascading link to Full Screen (1x1) in CP conferences, hence displaying the speaker of one conference to a full window in the video layout of the other conference.

  Set this flag to **NO** when cascading between an Collaboration Server and an MGC that is functioning as a Gateway, if the participant layouts on the MGC are not to be forced to 1X1.

- Setting the **AVOID_VIDEO_LOOP_BACK_IN_CASCADE** *System Flag* to **YES** (default) prevents the speaker's image from being sent back through the participant link from the cascaded conference. This can occur in cascaded conferences with conference layouts other than 1x1. It results in the speaker's own video image being displayed in the speaker's video layout.

This option is supported with:

— In *H.323, SIP* environments.

— For *Basic Cascading* of *Continuous Presence,* aconferences. If a *Master MCU* has two slave MCUs, participants connected to the slave MCUs will not receive video from each other.

— Video resolution will be according to the *Resolution Configuration*.

For more details on defining system flags, see "*Modifying System Flags"* on page **20-1**.

DTMF Forwarding

When two conferences are connected over an IP link, DTMF codes from one conference are not forwarded to the second conference with the exception of the following operations that are available throughout the conference and the forwarding of their DTMF codes is not suppressed (i.e. they will apply to both conferences):

- Terminate conference.
- Mute all but me.
- Unmute all but me.
- Secure conference.
- Unsecure conference.

During cascading between a gateway and a conference **all** DTMF codes are forwarded from the gateway to the conference and vice versa.

Play Tone Upon Cascading Link Connection

The Collaboration Server can be configured to play a tone when a cascading link between conferences is established. The tone is played in both conferences.

This tone is not played when the cascading link disconnects from the conferences.

The tone used to notify that the cascading link connection has been established cannot be customized.

The option to play a tone when the cascading link is established is enabled by setting the *System Flag*: **CASCADE_LINK_PLAY_TONE_ON_CONNECTION** to **YES**.

Default value: **NO**.

The tone volume is controlled by the same flag as the IVR messages and tones: **IVR_MESSAGE_VOLUME**.

Basic Cascading

In this topology, a link is created between two conferences, usually running on two different MCUs. The MCUs are usually installed at different locations (states/countries) to save long distance charges by connecting each participant to their local MCU, while only the link between the two conferences is billed as long distance call.

- When linking two conferences using an IP cascading link:
  - The destination MCU can be indicated by:
    - IP address
    - H.323 Alias
  - Both MCUs must be located in the same network.
- One MCU can be used as a gateway.

Basic Cascading using IP Cascaded Link

In this topology, both MCUs can be registered with the same gatekeeper or the IP addresses of both MCUs can be used for the cascading link. Content can be sent across the Cascading Link.
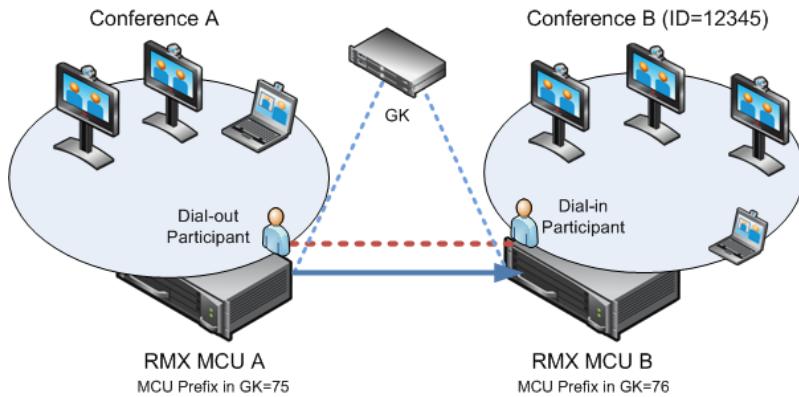
Figure 5-2 Basic Cascading Topology - IP Cascading Link

For example, MCU B is registered with the gatekeeper using 76 as the MCU prefix.

The connection between the two conferences is created when a dial out IP participant is defined (added) to conference A whose dial out number is the dial-in number of the conference or Entry Queue running on MCU B.

Dialing Directly to a Conference

Dial out IP participant in conference A dials out to the conference running on MCU B entering the number in the format:
[MCU B Prefix/IP address][conference B ID].

For example, if MCU B prefix is 76 and the conference ID is 12345, the dial number is **7612345**.

Dialing to an Entry Queue

When dialing to an Entry Queue, the dial out participant dials the MCU B prefix or IP address of MCU B and the Entry Queue ID in the format:
[MCU B Prefix/IP address][EQ B ID].

For example, if MCU B prefix is 76 and the Entry Queue ID is 22558, the dial number is **7622558**.

When the participant from conference A connects to the Entry Queue, the system plays to all the participants in Conference A the IVR message requesting the participant to enter the destination conference ID.

At this point, the Conference A organizer or any other participant in the conference can enter the required information for the IVR session using DTMF codes. For example, the meeting organizer enters the destination conference ID - **12345**.

Any DTMF input from conference A is forwarded to the Entry Queue on MCU B to complete the IVR session and enable the move of the participant to the destination conference B.

Once the DTMF codes are entered and forwarded to the Entry Queue on MCU B, the IVR session is completed, the participant moved to the destination conference and the connection between the two conferences is established.

Automatic Identification of the Cascading Link

In both dialing methods, the system automatically identifies that the dial in participant is an

MCU and creates a Cascading Link and displays the link icon for the participant ( ). The master-slave relationship is randomly defined by the MCUs during the negotiation process of the connection phase.

Suppression of DTMF Forwarding

Forwarding of the DTMF codes from one conference to another over an ISDN cascading link is not automatically suppressed as with IP cascading link and it can be limited to basic operations while suppressing all other operations by a system flag: DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS.

System Flag Settings

The **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS** flag determines the time period (in seconds) that MCU A will forward DTMF inputs from conference A participants to MCU B.

Once the timer expires, most of the DTMF codes (excluding five operations as for IP links) entered in conference A will not be forwarded to conference B. This is done to prevent an operation requested by a participant individually (for example, mute my line) to be applied to all the participants in conference B.

Flag range (in seconds): **0 - 360000**

This flag is defined on MCU A (the calling MCU).

If a flag is not listed in the *System Flags* list it must be added to the *system.cfg* file before it can be modified. For more details on defining system flags, see "*Modifying System Flags*" on page **20-1**.

Star Cascading Topology

In the Star topology (as well as in the Basic topology), the MCUs are usually installed at different locations (states/countries) and participants connect to their local MCU to facilitate the connection and save long distance call costs. Star Topology Cascading requires that all cascaded MCUs reside on the same network.

> Although participants in Star Cascading conferences can connect to their local conference using H.323, SIP and ISDN, the Cascading Links between conferences must connect via H.323.

Content sharing is available to all conferences over the H.323 Cascading Link.

In this topology, the MCUs are networked together using two modes:

• Master-Slave Cascading
• Cascading via Entry Queue

Master-Slave Cascading

It is similar to MIH (Multi Hierarchy) cascading, with only two levels: one *Master MCU* on level 1 and several *Slave* MCUs on level 2.

The cascading hierarchy topology can extend to four levels (Figure 5-5) and should be deployed according to the following guidelines:

- If an Collaboration Server is deployed on level 1:
  — Collaboration Server systems can be used on level 2
  — MGC with version 9.0.4 can be used on level 2 if Collaboration Server version 7.0.2 and higher is deployed in level 1
- If an *MGC* is deployed on level 1:
  — MGC or Collaboration Server can be used on level 2.
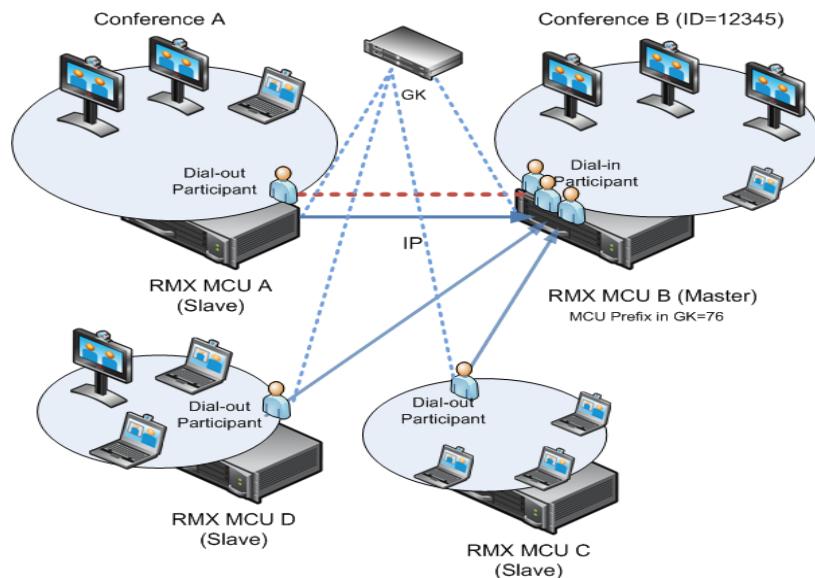
Figure 5-3 *Master-Slave Star Cascading Topology*

- When creating a cascading link between two Collaboration Servers:
  — The Collaboration Servers operate in CP (Continuous Presence) mode.
- When creating a cascading link between MGCs and Collaboration Servers:

The following table summarizes *Video Session Modes* line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

Table 1   *MIH Cascading – Video Session Mode and Line Rate*

Topology	MCU Type	Video Session Mode	Line Rate	Endpoint
Level 1	Collaboration Server	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s	HDX
Level 2	Collaboration Server			

Table 1   *MIH Cascading – Video Session Mode and Line Rate (Continued)*

Topology	MCU Type	Video Session Mode	Line Rate	Endpoint
Level 1	Collaboration Server	CP - CIF	768Kb/s, 2Mb/s	VSX
Level 2	Collaboration Server			
Level 1	MGC	CP - CIF 263	768Kb/s, 2Mb/s	HDX, VSX
Level 2	Collaboration Server	CP - CIF 264		
Level 1	MGC	VSW - HD	1.5Mb/s	HDX
Level 2	Collaboration Server	VSW HD		

To establish the links between two Collaboration Servers requires the following procedures be performed:

- Establish the Master-Slave relationships between the cascaded conferences by defining the dialing direction.
- Create the Master and Slave conferences, defining the appropriate line rate.
- Create a cascade-enabled *Dial-out Participant* link in the Master conference
- Create a cascade-enabled *Dial-in Participant* link in the Slave conference.

Creating a Cascade Enabled Dial-out/Dial-in Participant Link

The connection between two cascaded conferences is established by a cascade enabled dial-out and dial-in participants, acting as a cascades link.

The dialing direction determines whether the dial-out participant is defined in the conference running on the Master MCU or the Slave MCU. For example, if the dialing direction is from the Master conference on level 1 to the Slave conference on level 2, the dial-out participant is defined in the Master conference on level 1 and a dial-in participant is defined in the Slave conference running on the MCU on level 2.

If the cascade-enabled dial-out participant always connects to the same destination conference on the other (second) MCU, the participant properties can be saved in the Address Book of the MCU for future repeated use of the cascaded link.

To define the dial-out cascade participant link:

1   In the *Conferences* pane, select the conference.

2   In the *Participants* pane, click **New Participant** (🧑).

The *New Participant - General* dialog box is displayed.
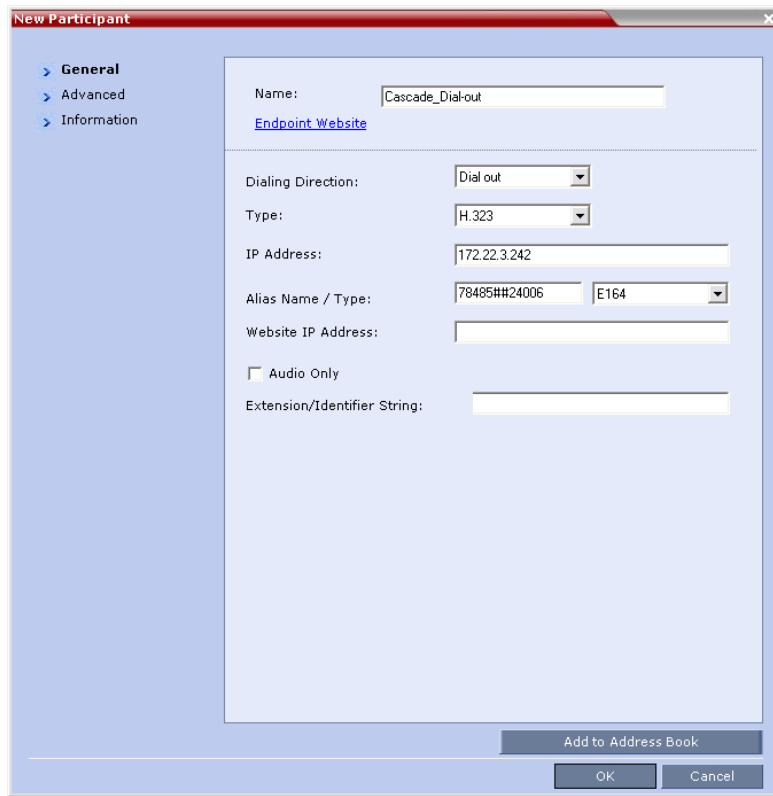
3 Define the following parameters:

Table 2 New Participant – Dial-out Cascade Link

Field	Description
Name	Enter the participant's name. This field may not be left blank. Duplicate participant names, comma, and semi-colon characters may not be used in this field.
Dialing Direction	Select **Dial-out**.
Type	Select **H.323**.
IP Address	Enter the IP address of the Signaling Host of the MCU running the other (second) conference, where the cascade enabled Entry Queue is defined.

Table 2 *New Participant – Dial-out Cascade Link (Continued)*

Field	Description
Alias Name	If you are using the target MCU IP address, enter the Conference ID of the target conference. For example: `24006` If a gatekeeper is used, instead of the IP address, you can enter the prefix of the target MCU as registered with the gatekeeper, as part of the dialing string and the conference ID in the format: **`<Target MCU Prefix>`**`<Conference_ID>` For example: **`925`**`24006` If the conference has a password and you want to include the password in the dial string, append the password to in the dial string after the Conference ID. For example: `92524006`**`##1234`** If the conference has a password and you do not want to include the password in the dial string, set the `ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD` flag to **YES**. For more information see *"Modifying System Flags"* on page **20-1**.
Alias Type	Select **E.164** (digits 0-9, *, #).

4   Click the *Advanced* tab.

5   In the *Cascade* field, select:

— **Slave**, if the participant is defined in a conference running on a Slave MCU.

— **Master**, if the participant is defined in a conference running on the Master MCU.

6   Click **OK**.

To define a Dial-in Participant as the cascade link:

This participant is added to the ongoing conference on the *Slave* MCU.

1 In the *Participants* list, click the **New Participant** button( ).

The *New Participant - General* dialog box opens.
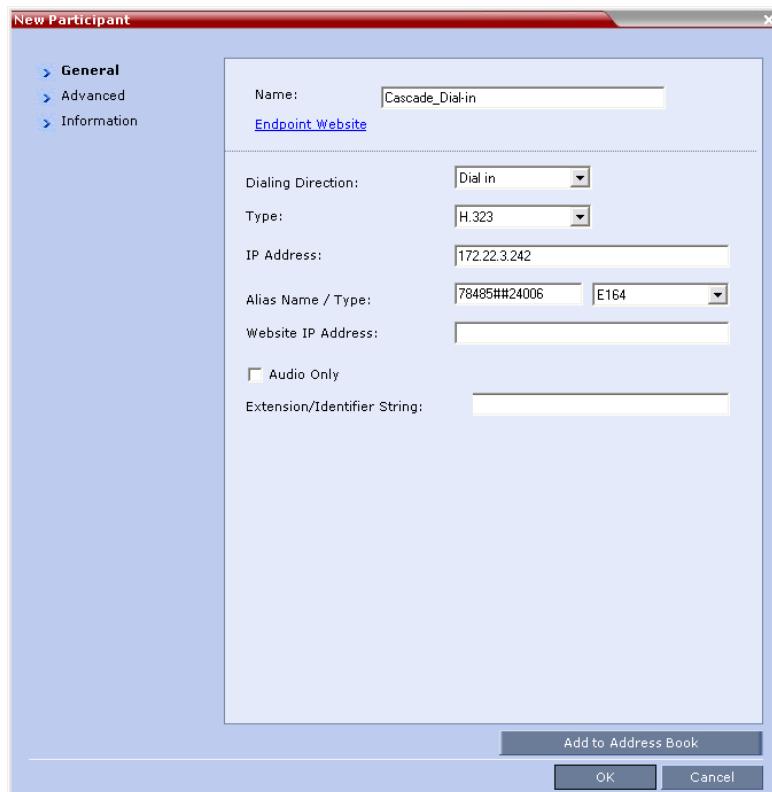
2 Define the following parameters:

Table 5-1 New Participant – Dial-in Cascade Link

Field	Description
Display Name	Enter the participant's name. This field may not be left blank. Duplicate participant names, comma, and semi-colon characters may not be used in this field.
Dialing Direction	Select **Dial-in**.
Type	Select **H.323**.
IP Address	**If a gatekeeper is used:** This field is left empty. **If a gatekeeper is not used:** Enter the IP address of the Signaling Host of the MCU running the other conference.
Alias Name	**If a gatekeeper is used:** Enter the name of the other (second) conference. **If a gatekeeper is not used:** Enter the ID of the MCU running the other (second) conference.

Table 5-1 New Participant – Dial-in Cascade Link (Continued)

Field	Description
Alias Type	**If a gatekeeper is used:** H.323 ID **If a gatekeeper is not used:** Select **E.164** (digits 0-9, *, #).

3 Click the **Advanced** tab.

The *Advanced* tab opens.
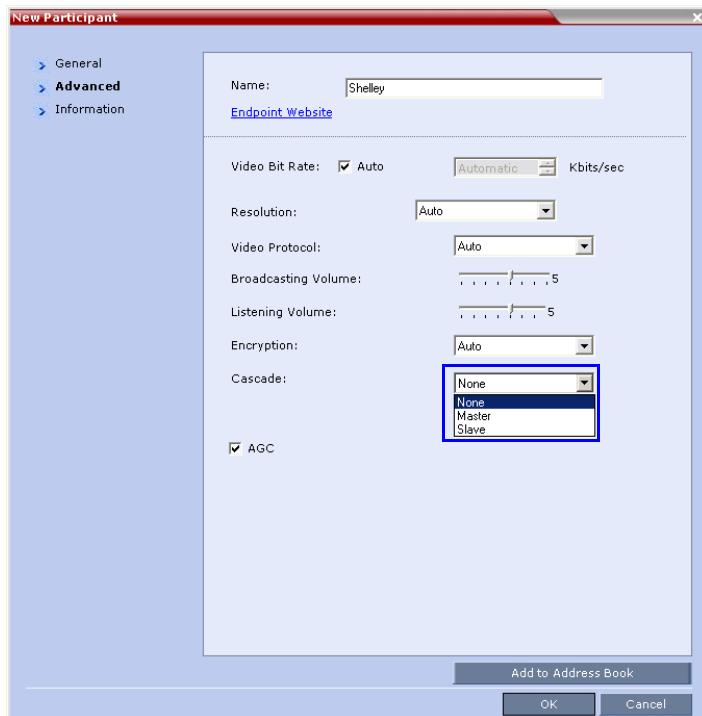
4 In the *Cascaded Link* field, select:

— **Slave**, if the participant is defined in a conference running on a Slave MCU.

— **Master**, if the participant is defined in a conference running on the Master MCU.

5 Click the **OK** button.

Monitoring Star Cascaded Conferences

To monitor both conferences at the same time, two instances of the Collaboration Server Web Clients must be opened (one for each MCU) by entering the IP Address of each MCU. If both conferences are running on the same MCU, only one Collaboration Server Web Client window is required.

When conferences are cascaded, the *Participant* list pane of each of the two conferences will display a linked icon ( ); a dial-in linked icon in the destination conference (Conference B) and a dial-out linked icon in the linked conference (Conference A).

The *Conferences* list panes in each of the two conferences will display a cascaded conference icon ( ) indicating that a conference running on the MCU is presently cascading with another conference running on the same or another MCU. The cascaded conference icon will be displayed for a short period of time and then disappear.

Conference A (Linked Conference)
Dial-out Linked Participant

Conference B (Destination Conference)
EQ created Dial-in Linked Participant

Cascaded conference icon

Cascading Conferences - H.239-enabled MIH Topology

H.239 Multi-Hierarchy (MIH) cascading is available to Collaboration Server users enabling them to run very large conferences on different MCUs in multiple levels of Master-Slave relationships using an H.323 connection.

Multi-Hierarchy (MIH) Cascading is implemented where the cascaded MCUs reside on different networks, whereas *Star Topology Cascading* requires that all cascaded MCUs reside on the same network.

MIH Cascading allows:

- Opening and using a content channel (H.239) during conferences.
- Full management of extremely large, distributed conferences.
- Connecting conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, for example, different communication protocols, such as, serial connections, ISDN, etc.
- Significant call cost savings to be realized by having participants call local MCUs which in turn call remote MCUs, long distance.

> Although participants in MIH Cascading conferences can connect using H.323, SIP and ISDN, the MIH Cascading Links must connect via H.323.

MIH Cascading Levels

The cascading hierarchy topology can extend to up to four levels (Figure 5-5), where the most common configuration includes up to three levels.
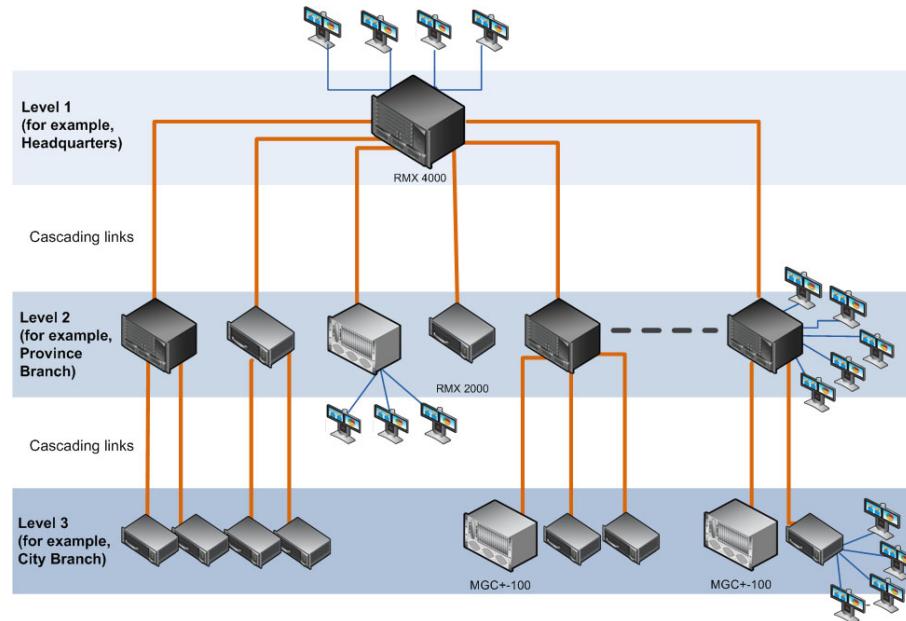
Figure 5-4 *MIH Cascade - a Sample 3-Level Cascading Configuration*

Cascading Topologies

The cascading hierarchy topology should be deployed according to the following guidelines:

- If an *RMX* is deployed on level 1 (recommended deployment):
    — Any *RMX* can be used on level 2, 3 and 4 (recommended deployment),
    — MGC version 9.0.4 can be used on level 2 and level 3,
    — *DST MCS 4000* and other MCUs can be deployed on levels 3 and 4.
- If an *MGC* is deployed on level 1:
    — *MGC* or *RMX* can be used on level 2,
    — *DST MCS 4000* and other MCUs can be deployed on levels 3 and 4.
- *DST MCS 4000 MCU*s connect as endpoints to the *RMX*s or *MGC*s on higher levels.
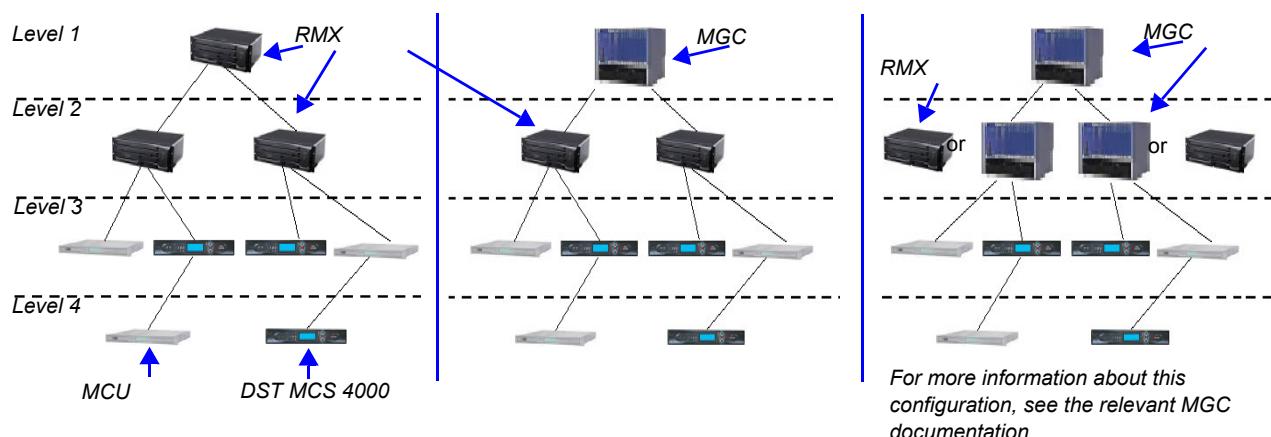
Figure 5-5 *MIH Cascade Levels*

MIH Cascading Guidelines in CP Licensing

Master - Slave Conferences

- It is recommended to have RMX systems at all levels to leverage the high quality video and content offered by the RMX.
- In *MIH Cascading* conferences, although there are multiple levels of Master and Slave relationships between conferences, the conference that runs on the MCU on level 1 of the hierarchy must be the Master for the entire cascading session. When an MGC is part of the cascading topology, it can be configured at any level if MGC Version 9.0.4 is installed, otherwise, it must be set as Level 1 MCU.
- Conferences running on MCUs on levels 2 and 3 and can be both Masters and Slaves to conferences running on MCUs on levels above and below them.
- All conferences running on MCUs on the lowest level in the configuration (for example, level 3 in a 3-level hierarchy configuration) are Slave conferences.
- When the DST MCS 4000 is on level 3 and acting as slave to level 2, the RMX on level 2 must dial out to it in order for the DST MCS 4000 to be identified as slave. The link between the two MCU (dial out participant) is defined as a standard participant and not as a cascading link.
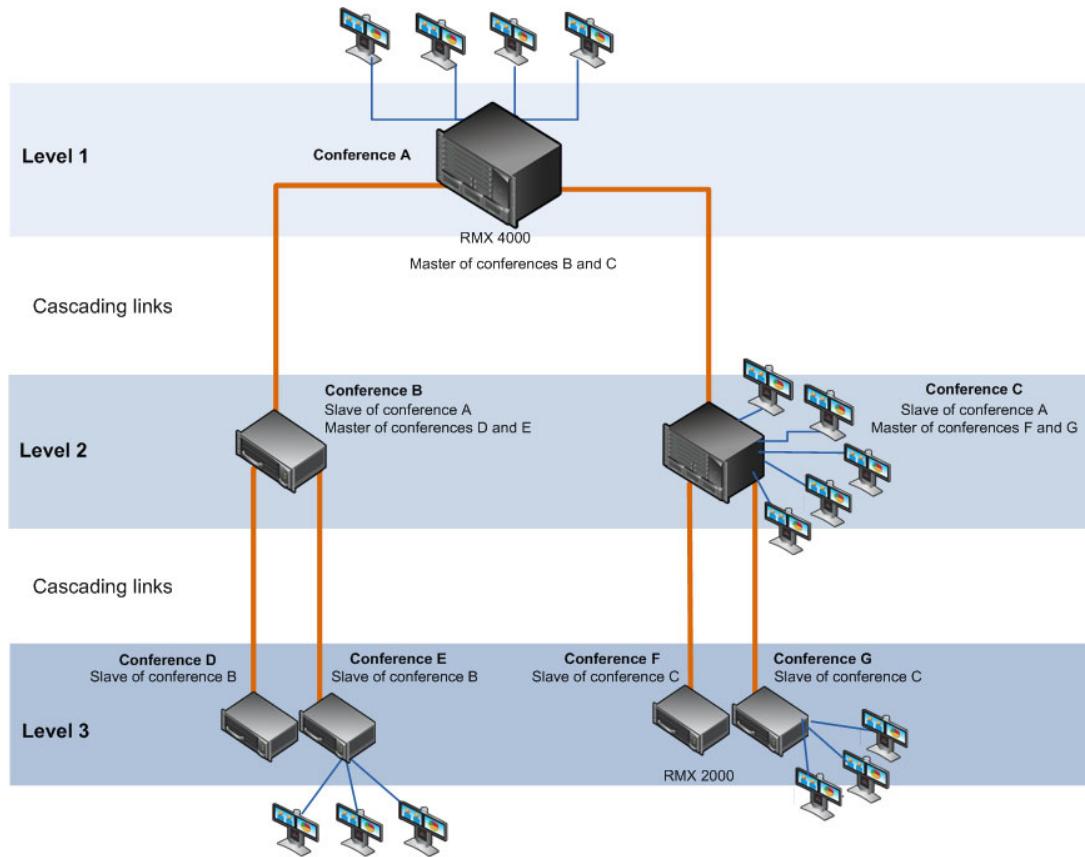
Figure 5-6 MIH Cascading – Master-Slave Relationship

Video Session Mode, Line Rate and Video Settings

The types of MCUs, their position in the cascade topology and the endpoint capabilities (HD/CIF and H.263/H.264) determine the *Video Session Type* of the *MIH Cascading* conference.

- When creating a cascading link between two RMXs:
  - The RMXs operate in CP (Continuous Presence) mode.
  - DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between MGCs and RMXs:
  - If there are no MGCs on level 2, the MGCs can operate in either in CP or VSW (Video Switching) mode.
  - If there are MGCs on level 2, the MGCs can only operate in VSW mode.
  - MGC does not support H.264 High Profile, therefore when MGC is part of the Cascading topology, do not select *High Profile* on the RMX system.
  - DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between two MGCs:
  - The MGCs must be configured to operate in VSW mode.

For more details about the MGC to MGC connection, see the *MGC Manager User's Guide, Volume II, Chapter 1, "Ad Hoc Auto Cascading and Cascading Links"*.

- To enable the connection of the links between cascaded conferences, they must run at the same line rate.
- To enable Content sharing between the RMX and the MGC, the rate allocated to the content must be identical in both conferences. Make sure that the line rate set for both conferences, and the Content Settings (Graphics, Hi-res Graphics or Live video) are selected correctly to ensure the compatible rate allocation. For more details on the RMX rate allocation to the Content channel, see "*SIP BFCP Content Capabilities*" on page **4-2**.

The following table summarizes *Video Session Modes* line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

Table 5-2   MIH Cascading – Video Session Mode and Line Rate

Topology	MCU Type	Video Session Type	Line Rate
Level 1	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 2	RMX		
Level 1	RMX	CP - CIF	768Kb/s, 2Mb/s
Level 2	RMX		
Level 1	RMX	CP	768Kb/s, 2Mb/s
Level 2	MGC	CP or VSW	
Level 1	MGC	CP - CIF 263	768 kb/s, 2Mb/s
Level 2	RMX	CP - CIF 264	
Level 1	MGC	VSW - HD	1.5Mb/s
Level 2	RMX	VSW HD	
Level 2	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	RMX		
Level 2	MGC	VSW*	384 kbps, 768 kbps
Level 3	MGC		
Level 2	RMX	CP/VSW -HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	MCS 4000		
Level 2	RMX	CP - CIF	768kb/s, 2Mb/s
Level 3	MCS 4000		

* When MGC is on Level 3, Content cannot be shared between Level 2 and Level 3.

Video Layout in Cascading CP Conferences

Cascade links are treated as endpoints in CP conferences and are allocated resources according to "*Default Minimum Threshold Line Rates and Resource Usage Summary*" on page **3-9**. Cascaded links in 1x1 video layout are in SD resolution.

When cascading two conferences, the video layout displayed in the cascaded conference is determined by the selected layout in each of the two conferences. Each of the two conferences will inherit the video layout of the other conference in one of their windows.

In order to avoid cluttering in the cascaded window, it is advised to select appropriate video layouts in each conference before cascading them.

	Conference A	Conference B
Without Cascade		
During Cascading		

Video layout of Conf. B in window of Conf. A

Video layout of Conf. A in window of Conf. B
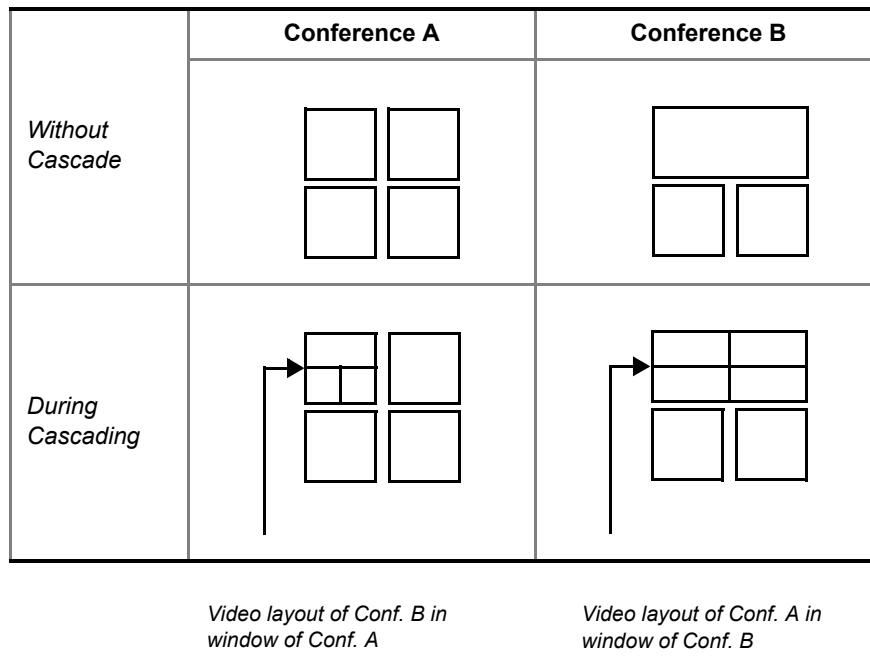
Figure 5-7 *Video Layouts in Cascaded Conferences*

Guidelines

To ensure that conferences can be cascaded and video can be viewed in all conferences the following guidelines are recommended:

• The same version installed on all MCUs participating the cascading topology
• The same license installed on all MCUs participating the cascading topology
• Same Conference Parameters are defined in the Profile of the conferences participating in the cascading topology
  — Conference line rates should be identical
  — Content rate should be identical
  — Same encryption settings
• DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences
• DTMF forwarding is suppressed
• The video layout of the link is set to 1x1 by the appropriate system flag.

Flags controlling Cascade Layouts

• Setting the **FORCE_1X1_LAYOUT_ON_CASCADED_LINK _CONNECTION** *System Flag* to **YES** (default) automatically forces the cascading link to Full Screen (1x1) in CP conferences, hence displaying the speaker of one conference to a full window in the video layout of the other conference.

  Set this flag to **NO** when cascading between an RMX and an MGC that is functioning as a Gateway, if the participant layouts on the MGC are not to be forced to 1X1.

- Setting the **AVOID_VIDEO_LOOP_BACK_IN_CASCADE** *System Flag* to **YES** (default) prevents the speaker's image from being sent back through the participant link from the cascaded conference. This can occur in cascaded conferences with conference layouts other than 1x1. It results in the speaker's own video image being displayed in the speaker's video layout.

  This option is supported with:

  — In *H.323, SIP* and *ISDN* environments.

  — For *Basic Cascading* of *Continuous Presence* and *Video Switched* conferences. If a *Master MCU* has two slave MCUs, participants connected to the slave MCUs will not receive video from each other.

  — Video resolution will be according to the *Resolution Configuration*, or *VSW* profile.

For more details on defining system flags, see "*Modifying System Flags*" on page **20-1**.

6

Meeting Rooms

A Meeting Room is a conference saved on the MCU in passive mode, without using any of the system resources. A Meeting Room is automatically activated when the first participant dials into it. Meeting Rooms can be activated as many times as required. Once activated, a Meeting Room functions as any ongoing conference.

In AVC CP Conferences, dial-out participants can be connected to the conference automatically, or manually. In the automatic mode the system calls all the participants one after the other. In the manual mode, the Collaboration Server user or meeting organizer instructs the conferencing system to call the participant. Dial-out participants must be defined (mainly their name) and added to the conference. This mode can only be selected at the conference/Meeting Room definition stage and cannot be changed once the conference is ongoing.

A Meeting Room can be designated as a Permanent Conference. For more information see *"]Audio Algorithm Support"* on page **4-45**.

The maximum of number of Meeting Rooms that can be defined is 1000.

The system is shipped with four default Meeting Rooms as shown in Table 6-1.

Table 6-1   Default Meeting Rooms List

Meeting Room Name	ID	Default Line Rate
Maple_Room	1001	384 Kbps
Oak_Room	1002	384 Kbps
Juniper_Room	1003	384 Kbps
Fig_Room	1004	384 Kbps

Meeting Rooms List

Meeting Rooms are listed in the *Meeting Room* list pane.

To list Meeting Rooms:

>> In the *RMX Management* pane, in the *Frequently Used* list, click the **Meeting Rooms** button 🗄.

The *Meeting Rooms List* is displayed.

Meeting Room Toolbar   Meeting Room List

Access to Meeting Rooms
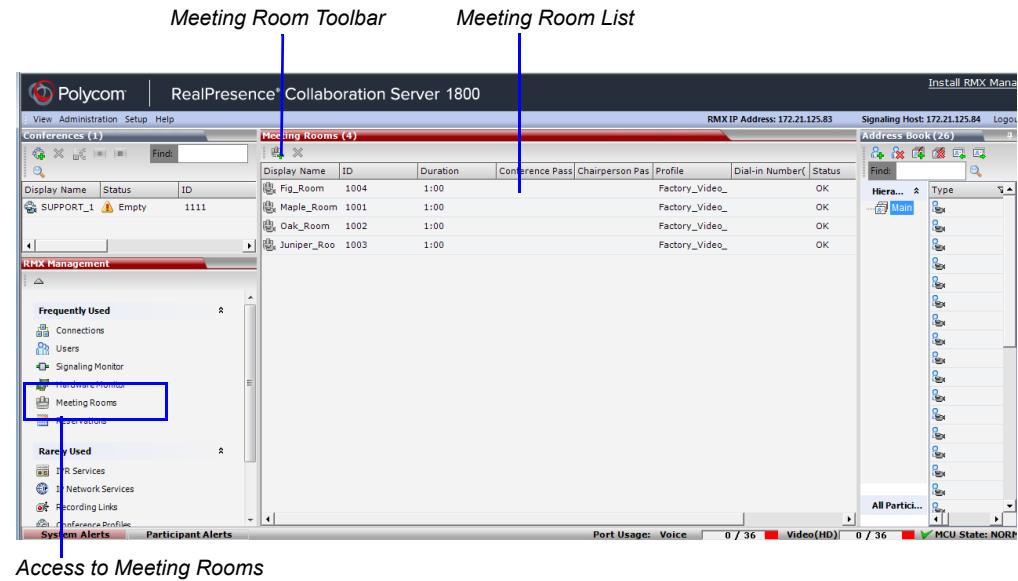
An active Meeting Room becomes an ongoing conference and is monitored in the same way as any other conference.

The *Meeting Room List* columns include:

Table 6-2   Meeting Rooms List Columns

Field	Description
Display Name	Displays the name and the icon of the Meeting Room in the *Collaboration Server Web Client*.
	(green) — An active video Meeting Room that was activated when the first participant connected to it.
	(gray) — A passive video Meeting Room that is waiting to be activated.
ID	Displays the Meeting Room ID. This number must be communicated to H.323 conference participants to enable them to dial in.
Duration	Displays the duration of the Meeting Room in hours using the format HH:MM (default 01:00).

Table 6-2   Meeting Rooms List Columns (Continued)

Field	Description	
Conference Password	The password to be used by participants to access the Meeting Room. If blank, no password is assigned to the conference. This password is valid only in conferences that are configured to prompt for a conference password in the IVR Service.	The Collaboration Server can be configured to automatically generate conference and chairperson passwords when these fields are left blank.
Chairperson Password	Displays the password to be used by the users to identify themselves as *Chairpersons.* They are granted additional privileges. If left blank, no chairperson password is assigned to the conference. This password is valid only in conferences that are configured to prompt for a chairperson password.	
Profile	Displays the name of the Profile assigned to the Meeting Room. For more information, see "*Defining New Profiles"* on page **2-9**.	
SIP Registration	The status of registration with the SIP server: • **Not configured** - Registration with the SIP Server was not enabled in the Conference Profile assigned to this conferencing Entity. In Multiple Networks configuration, If one service is not configured while others are configured and registered, the status reflects the registration with the configured Network Services. The registration status with each SIP Server can be viewed in the *Properties - Network Services* dialog box of each conferencing entity. When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with an URL derived from its own signaling address. • **Failed** - Registration with the SIP Server failed. This may be due to incorrect definition of the SIP server in the IP Network Service, or the SIP server may be down, or any other reason the affects the connection between the Collaboration Server or the SIP Server to the network. • **Registered** - the conferencing entity is registered with the SIP Server. • **Partially Registered** - This status is available only in Multiple Networks configuration, when the conferencing entity failed to register to all the required Network Services if more than one Network Service was selected.	

Meeting Room Toolbar & Right-click Menu

The Meeting Room toolbar and right-click menus provide the following functionality:

Table 6-3   Meeting Room Toolbar and Right-click Menus

Toolbar button	Right-click menu	Description
	New Meeting Room	Select this button to create a new Meeting Room.

Table 6-3   Meeting Room Toolbar and Right-click Menus

Toolbar button	Right-click menu	Description
✖	*Delete Meeting Room*	Select any Meeting Room and then click this button to delete the Meeting Room.

Dial out to AVC participants assigned to a Meeting Room will only start when the dial in participant who has activated it has completed the connection process and the Meeting Room has become an ongoing conference.

Creating a New Meeting Room

To create a new meeting room:

>> In the *Meeting Rooms* pane, click the **New Meeting Room** 📋 button *or* right-click an empty area in the pane and then click **New Meeting Room**.

The *New Meeting Room* dialog box is displayed.
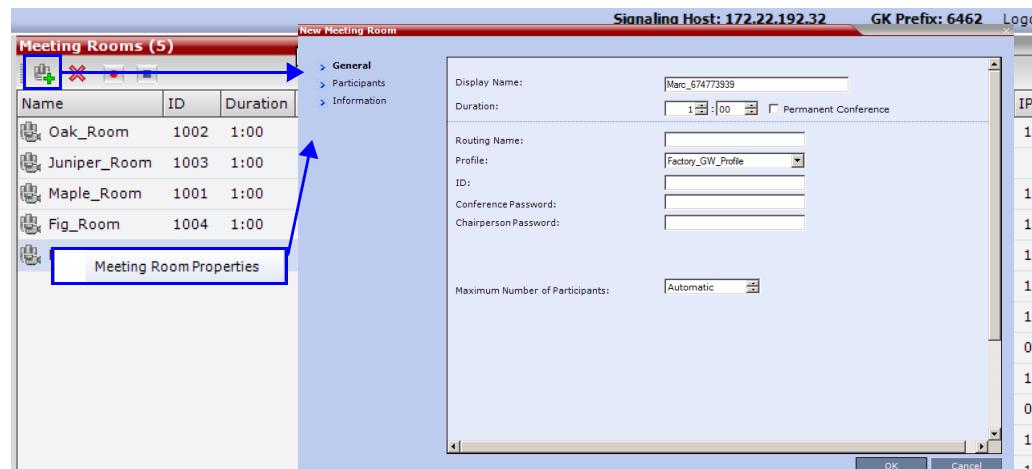
The definition procedure is the same as for the new conference.

If SIP Factories are being used do not assign a Meeting Room the ID 7001. This ID is reserved for the default SIP Factory.

For more information, see the *Polycom RMX 1800 Getting Started Guide, "Starting a Conference from the Conferences Pane"* on page **3-12**.

7

Entry Queues, Ad Hoc Conferences and SIP Factories

Entry Queues

An Entry Queue (EQ) is a special routing lobby to access conferences. Participants connect to a single-dial lobby and are routed to their destination conference according to the Conference ID they enter. The Entry Queue remains in a passive state when there are no callers in the queue (in between connections) and is automatically activated once a caller dials its dial-in number.

The maximum of number of Entry Queues that can be defined is 40.

The parameters (bit rate and video properties) with which the participants connect to the Entry Queue and later to their destination conference are defined in the Conference Profile that is assigned to the Entry Queue. For example, if the Profile Bit Rate is set to 384kbps, all endpoints connect to the Entry Queue and later to their destination conference using this bit rate even if they are capable of connecting at higher bit rates.

An *Entry Queue IVR Service* must be assigned to the Entry Queue to enable the voice prompts guiding the participants through the connection process. The Entry Queue IVR Service also includes a video slide that is displayed to the participants while staying in the Entry Queue (during their connection process).

Different Entry Queues can be created to accommodate different conferencing modes, conferencing parameters (by assigning different Profiles) and prompts in different languages (by assigning different *Entry Queue IVR Services*).

For more information, see "*IVR Services List*" on page **15-1**.

The Entry Queue can also be used for Ad Hoc conferencing. If the Ad Hoc option is enabled for the Entry Queue, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID. For more information about Ad Hoc conferencing, see "*Ad Hoc Conferencing*" on page **7-9**.

An Entry Queue can be designated as Transit Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred. For more information, see "*Transit Entry Queue*" on page **7-5**.

Default Entry Queue properties

The system is shipped with a default Entry Queue whose properties are:

Table 7-1   Default Entry Queue Properties

Parameter	Value
Display Name	DefaultEQ The user can change the name if required.
Routing Name	DefaultEQ The default *Routing Name* cannot be changed.
ID	1000
Profile name	Factory_Video_Profile. Profile Bit Rate is set to 384 Kbps.
Entry Queue Service	Entry Queue IVR Service. This is default Entry Queue IVR Service shipped with the system and includes default voice messages and prompts in English.
Ad Hoc	Enabled

Defining a New Entry Queue

You can modify the properties of the default Entry Queue and define additional Entry Queues to suit different conferencing requirements.

To define a new Entry Queue:

1   In the *RMX Management - Rarely Used* pane, click **Entry Queues**.
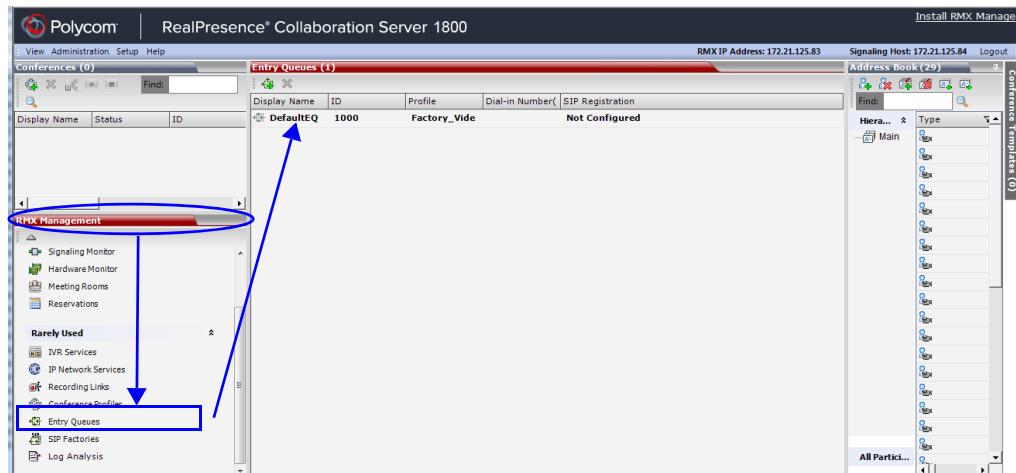
2 In the *Entry Queues* list pane, click the **New Entry Queue** button.
The *New Entry Queue* dialog box opens.
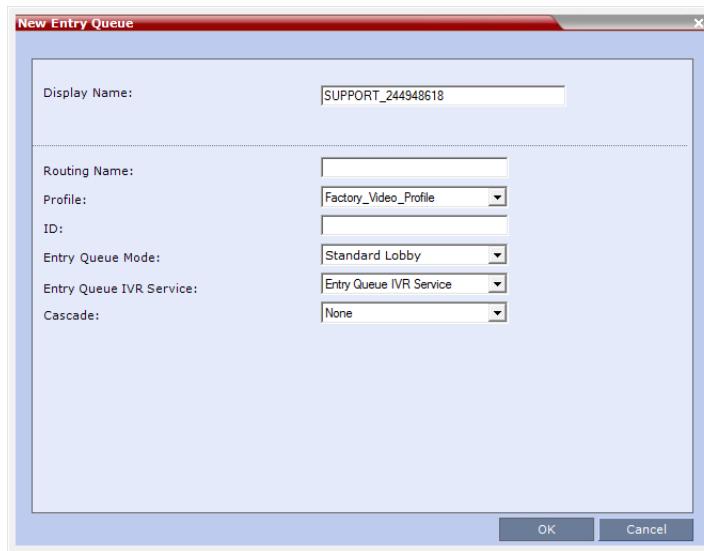
3 Define the following parameters:

Table 7-2: Entry Queue Definitions Parameters

Option	Description
Display Name	The Display Name is the conferencing entity name in native language character sets to be displayed in the Collaboration Server Web Client. In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the *Display Name* field that can be modified using Unicode encoding. • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message requesting you to enter a different name.
Routing Name	Enter a name using ASCII text only. If no *Routing Name* is entered, the system automatically assigns a new name as follows: • If an all ASCII text is entered in *Display Name*, it is used also as the *Routing Name.* • If any combination of Unicode and ASCII text (or full Unicode text) is entered in *Display Name*, the *ID* (such as Conference ID) is used as the *Routing Name.*

Table 7-2: Entry Queue Definitions Parameters (Continued)

Option	Description
Profile	Select the Profile to be used by the Entry Queue. The default Profile is selected by default. This Profile determines the Bit Rate and the video properties with which participants connect to the Entry Queue and destination conference. In Ad Hoc conferencing, it is used to define the new conference properties.
ID	Enter a unique number identifying this conferencing entity for dial in. Default string length is 4 digits. If you do not manually assign the ID, the MCU assigns one after the completion of the definition. The ID String Length is defined by the flag NUMERIC_CONF_ID_LEN in the System Configuration.
Entry Queue Mode	Select the mode for the Entry Queue:
	Standard Lobby (default)-When selected, the Entry Queue is used as a routing lobby to access conferences. Participants connect to a single-dial lobby and are routed to their destination conference according to the Conference ID they enter.
	Ad Hoc - Select this option to enable the Ad Hoc option for this Entry Queue. In this mode, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID.
	IVR Service Provider Only - Not Supported with Polycom RMX 1800*.*
	External IVR Control - Not Supported with Polycom RMX 1800.
Entry Queue IVR Service	The default Entry Queue IVR Service is selected. If required, select an alternate Entry Queue IVR Service, which includes the required voice prompts, to guide participants during their connection to the Entry Queue.

4   Click **OK**.

The new *Entry Queue* is added to the *Entry Queues* list.

Listing Entry Queues

To view the list of Entry Queues:

>> In the *RMX Management - Rarely Used* pane, click **Entry Queues**.

The *Entry Queues* are listed in the *Entry Queues* pane.

You can double-click an Entry Queue to view its properties.

Modifying the EQ Properties

To modify the EQ:

>> In the *Entry Queues* pane, either double-click or right-click and select **Entry Queue Properties** of the selected *Entry Queue* in the list.

The Entry Queue Properties dialog box is displayed. All the fields may be modified except **Routing Name**.

Transit Entry Queue

A *Transit Entry Queue* is an Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred.

IP Calls are routed to the *Transit Entry Queue* when:

- A gatekeeper is not used, or where calls are made directly to the Collaboration Server's *Signaling IP Address*, with incorrect or without a Conference ID.
- When a gatekeeper is used and only the prefix of the Collaboration Server is dialed, with incorrect or without a Conference ID.
- When the dialed prefix is followed by an incorrect conference ID.

When no *Transit Entry Queue* is defined, all calls containing incomplete or incorrect conference routing information are rejected by the Collaboration Server.

In the *Transit Entry Queue*, the *Entry Queue IVR Service* prompts the participant for a destination conference ID. Once the correct information is entered, the participant is transferred to the destination conference.

Setting a Transit Entry Queue

The Collaboration Server factory default settings define the *Default Entry Queue* also as the *Transit Entry Queue*. You can designate another Entry Queue as the *Transit Entry Queue*.

Only one *Transit Entry Queue* may be defined per Collaboration Server and selecting another Entry Queue as the *Transit Entry Queue* automatically cancels the previous selection.

To designate an Entry Queue as Transit Entry Queue:

1 In the *Collaboration Server Management - Rarely Used* pane, click **Entry Queues**.

2 In the *Entry Queues* list, right-click the Entry Queue entry and then click **Set Transit Entry Queue**.
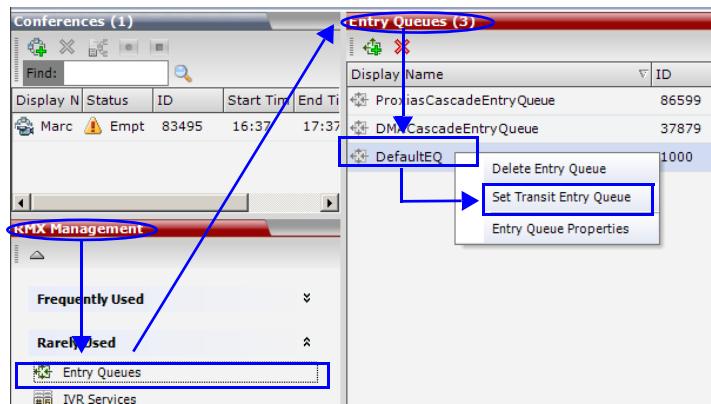
The Entry Queue selected as *Transit Entry Queue* is displayed in bold.

To cancel the Transit Entry Queue setting:

1 In the *Collaboration Server Management - Rarely Used* pane click **Entry Queues**.

2 In the *Entry Queues* list, right-click the *Transit Entry Queue* entry and then click **Cancel Transit Entry Queue**.

SIP Factories

A SIP Factory is a conferencing entity that enables SIP endpoints to create Ad Hoc conferences. The system is shipped with a default SIP Factory, named DefaultFactory.

> The default SIP Factory uses the conferencing ID 7001. If a SIP Factory is being used do not assign this ID to any conferencing entity, including conferences, reservations, and meeting rooms.

When a SIP endpoint calls the SIP Factory URI, a new conference is automatically created based on the Profile parameters, and the endpoint joins the conference.

The SIP Factory URI must be registered with the SIP server to enable routing of calls to the SIP Factory. To ensure that the SIP factory is registered, the option to register *Factories* must be selected in the Default IP Network Service.

The maximum of number of SIP Factories that can be defined is 40.

Creating SIP Factories

To create a new SIP Factory:

1 In the *RMX Management - Rarely Used* pane, click **SIP Factories**.

2 In the *SIP Factories* list pane, click the **New SIP Factory** button.
The *New Factory* dialog box opens.

3 Define the following parameters:

Table 7-3: New Factory Properties

Option	Description
Display Name	Enter the SIP Factory name that will be displayed. The Display Name is the conferencing entity name in native language character sets to be displayed in the Collaboration Server Web Client. In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the *Display Name* field that can be modified using Unicode encoding. • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message requesting you to enter a different name.
Routing Name	The *Routing Name* is defined by the user, however if no *Routing Name* is entered, the system will automatically assign a new name when the Profile is saved as follows: • If an all ASCII text is entered in *Display Name*, it is used also as the *Routing Name.* • If any combination of Unicode and ASCII text (or full Unicode text) is entered in *Display Name*, the *ID* (such as Conference ID) is used as the *Routing Name.*
Profile	The default Profile is selected by default. If required, select the conference Profile from the list of Profiles defined in the MCU. A new conference is created using the parameters defined in the Profile.
Automatic Connection	Select this check box to immediately accept the conference creator endpoint to the conference. If the check box is cleared, the endpoint is redirected to the conference and then connected.

4 Click **OK**.
The new SIP Factory is added to the list.

Monitoring Registration Status

The *SIP* registration status can be viewed in the *Entry Queue* or *SIP Factory* list panes.

The following statuses are displayed:

- **Not configured** - *Registration* with the *SIP* Server was not enabled in the *Conference Profile* assigned to the *Entry Queue* or *SIP Factory*.

  When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with an URL derived from its own signaling address.

- **Failed** - *Registration* with the *SIP Server* failed.
  This may be due to incorrect definition of the *SIP* server in the *IP Network Service*, or the *SIP Server* may be down, or any other reason the affects the connection between the Collaboration Server or the *SIP Server* to the network.

- **Registered** - the conferencing entity is registered with the *SIP Server*.

- **Partially Registered** - This status is available only in *Multiple Networks* configuration, when the conferencing entity failed to register to all the required *Network Services* if more than one *Network Service* was selected for *Registration*.

Ad Hoc Conferencing

The Entry Queue can also be used for Ad Hoc conferencing. If the Ad Hoc option is enabled for the Entry Queue, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID. The conference parameters are based on the Profile linked to the Entry Queue. As opposed to Meeting Rooms, that are predefined conferences saved on the MCU, Ad Hoc conferences are not stored on the MCU. Once an Ad Hoc conference is started it becomes an ongoing conference, and it is monitored and controlled as any standard ongoing conference.

For more information about Ad Hoc conferencing, see *Appendix D, "Ad Hoc Conferencing"* on page **D-1**.

Address Book

The Address Book stores information about the people and businesses you communicate with. The Address Book stores, among many other fields, IP addresses, phone numbers and network communication protocols used by the participant's endpoint. By utilizing the Address Book you can quickly and efficiently assign or designate participants to conferences. Groups defined in the Address Book help facilitate the creation of conferences. Participants can be added to the Address Book individually or in Groups.

The maximum of number of Address Book entries that can be defined on the Collaboration Server is 4000.

The Address Book can be organized into a multi-level hierarchical structure. It can be used to mirror the organizational layout of the enterprises and it is especially suitable for large-scale enterprises with a considerable number of conference participants and organizational departments and divisions. Groups in the Address Book can contain sub-groups or sub-trees, and individual address book participant entities.

The Address Book provides flexibility in arranging conference participants into groups in multiple levels and the capabilities to add groups or participants, move or copy participants to multiple groups within the address book, and use the address book to add groups and participants to a conference or *Conference Template*.

Importing and exporting of Address Books enables organizations to seamlessly distribute up-to-date Address Books to multiple Collaboration Server units.

Viewing the Address Book

You can view the participants currently defined in the Address Book. The first time the *Collaboration Server Web Client* is accessed, the *Address Book* pane is displayed.

Anchor Pin
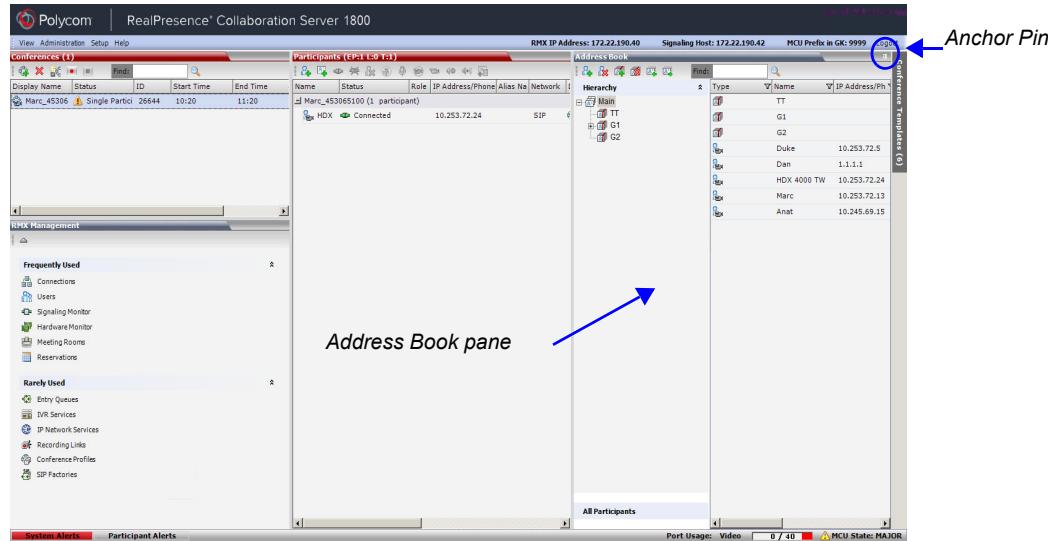
Address Book pane

The *Address Book* contains two panes:

• *Navigation pane* - contains the hierarchical tree and *All Participants* list

• *List pane* - displays the list of all the members of the selected group and sub-groups.

List pane
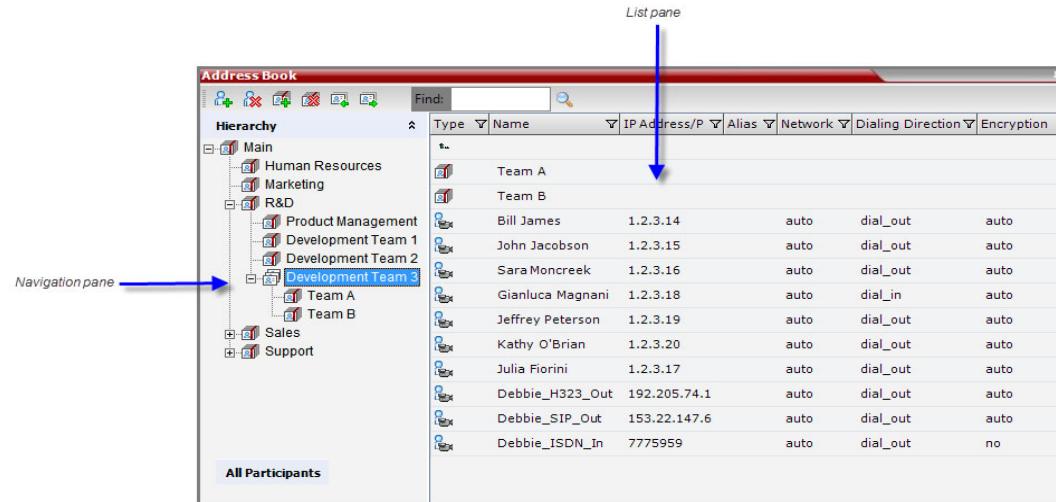
Navigation pane

The *Navigation pane* of the *Address Book* contains the following types of lists:

• **Hierarchical —** displays a multi-level hierarchical tree of groups and participants. Double-clicking a group on the navigation pane displays the group participants and sub-groups in the *List* pane.

• **All Participants —** double-clicking this selection displays the single unique entity of all the participants in a single level. When adding a participant to a group, the system adds a link to the participant's unique entity that is stored in the All Participants list. The same participant may be added to many groups at different levels, and all these

participant links are associated with the same definition of the participant in the *All Participants* list. If the participant properties are changed in one group, they will be changed in all the groups accordingly.

Displaying and Hiding the Group Members in the Navigation Pane

The currently selected group, whose group members are displayed in the Address Book List pane is identified by a special icon .

To expand the group to view the group members:

>> Double-click the group name or click the **Expand** button.

The address book entities and sub-groups of the group is displayed in the right group list pane. You can drill down the sub-group to view address book entities in the sub-group.

To move up to the next level and view the members in the upper level:

>> Double-click the **navigation arrow** button in the group members pane.

To collapse a group:

>> Double-click the group name or click the **Collapse** button.

Participants List Pane Information

The *Participants List* pane displays the following information for each participant:
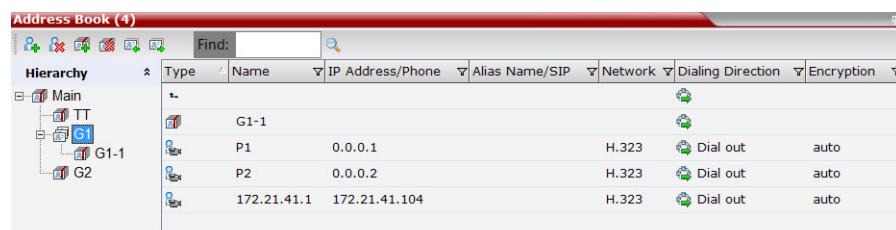
Table 8-1   Docked Address Book List Columns

Field/Option	Description
Type	Indicates whether the participant is a video ( ) or voice ( ).
Name	Displays the name of the participant.
IP Address/Phone	Enter the IP address of the participant's endpoint. • For H.323 participant define either the endpoint IP address or alias. For SIP participant define either the endpoint IP address or the SIP address.
Network	The network communication protocol used by the endpoint to connect to the conference: *H.323* or *SIP* .
Dialing Direction	*Dial-in* – The participant dials in to the conference. *Dial-out* – The Collaboration Server dials out to the participant.

Table 8-1   *Docked Address Book List Columns (Continued)*

Field/Option	Description
Encryption	Displays whether the endpoint uses encryption for its media. The default setting is *Auto*, indicating that the endpoint must connect according to the conference encryption setting.

For information on adding and modifying participants in the Address Book, see "*Managing the Address Book*" on page **8-7**.

Displaying and Hiding the Address Book

The Address Book can be hidden it by clicking the anchor pin (⬚) button in the pane header. The *Address Book* pane closes and a tab is displayed at the right edge of the screen.

>>   Click the tab to re-open the *Address Book*.

Click tab to open Address Book

Adding Participants from the Address Book to Conferences

You can add individual participants or a group of participants from the Address Book to a conference.

Adding Individual Participants from the Address Book to Conferences

You can add a participant or multiple participants to a new conference, ongoing conferences, or to *Conference Templates* by using the drag-and-drop operation.

> Multiple selection of group levels is not available.

To add a participant to a new conference or an ongoing conference:

1   In the *Address Book Navigation* pane, select the group from which to add participants.

2   In the *Address Book List* pane, select the participant or participants you want to add to the conference.

3   Click and hold the left mouse button and drag the selection to the Participants pane of the conference.

The participants are added to the conference.

Adding a Group from the Address Book to Conferences

You can add a group of participants to a new conference, ongoing conferences, or to *Conference Templates* by using the drag-and-drop operation.

To add a group to a new conference or an ongoing conference:

1 In the *Address Book Navigation* pane, select the group you want to add to the conference.

2 Click and hold the left mouse button and drag the selection to the *Participants* pane of the conference.

The participants in the group level and all sub-levels are added to the conference.

Participant Groups

A group is a predefined collection of participants. A group provides an easy way to manage clusters of participants that are in the same organizational structure and to connect a combination of endpoints to a conference. For example, if you frequently conduct conferences with the marketing department, you can create a group called "Marketing Team" that contains the endpoints of all members of the marketing team.

Groups can contain participants and sub-groups. You can define up to ten levels in the "Main" group.

Managing Groups in the Address Book

To manage the groups in the Address Book:

1   In the *Address Book Navigation* pane, right-click the group you want to manage.

The *Groups* menu is displayed.
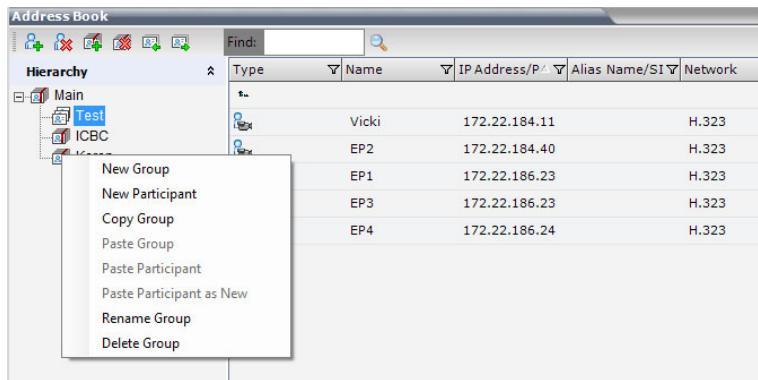
2   Select one of the following actions:

Table 8-2   Groups Drop-down Menu Actions

Action	Description
New Group	Creates a new group within the current group.
New Participant	Adds a new participant within the current group.
Copy Group	Copies the current group to be pasted as an additional group.
Paste Group	Places the copied group into the current group. The group name of the copied group is defined with "*Copy*" at the end of the group name. This action is only available after a **Copy Group** action has been implemented.
Paste Participant	Places the copied participant into the current selected group. This action is available after a **Copy** or **Cut** action was activated when selecting a single participant or multiple participants.
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds "*Copy*" at the end of the participant name. This action is only available after a **Copy** action was activated for a single participant.
Rename Group	Renames the group name.

Table 8-2   Groups Drop-down Menu Actions (Continued)

Action	Description
Delete Group	Deletes the group and all of its members. This action displays a message requesting confirmation to delete the group and all members connected with the group.

Additionally, you can drag a group from one location in the Address Book to another location, moving the group and all its members, including sub-groups, to its new location using the drag-and-drop operation. Moving a group to a new location can be done in the navigation pane or the list pane.

To drag a group from a location in the address book to another location:

1   Select the group you want to move.

2   Click and hold the left mouse button and drag the selection to the new location. The new location can be either the "Main" root level or another group level.

The group and all its members (participants and groups) are moved to the new address book location.

Managing the Address Book

Guidelines

- The multi-level *Address Book* can only be used in a local configuration on the Collaboration Server. The hierarchical structure cannot be implemented with the *Global Address Book* (GAB).
- Up to ten levels can be defined in the hierarchical structure of the Address Book.
- The default name of the root level is "Main". The "Main" root level cannot be deleted but the root level name can be modified.
- Address Book names support multilingual characters.
- Participants in the *Address Book* can be copied to multiple groups. However, only one participant exists in the *Address Book*. Groups that contain the same participants refer to the same definition of the participant entity.

Adding a Participant to the Address Book

Adding participants to the Address Book can be performed by the following methods:

- Directly in the Address Book.
- Moving or saving a participant from an ongoing conference to the Address Book.

When adding dial-out participants to the ongoing conference, the system automatically dials out to the participants using the Network Service defined for the connection in the participant properties.

Adding a New participant to the Address Book Directly

You can add a new participant to the "Main" group or to a group in the *Address Book*. Additionally, you can add a participant from a new conference, ongoing conference, or *Conference Template*.

To add a new participant to the Address Book:

1   In the *Address Book - Navigation* pane, select the group to where you want to add the new participant.

2   Click the **New Participant** button (⬚) or right-click the group to where you want to add the participant and select the **New Participant** option.

—   Alternatively, click anywhere in the *List* pane and select the **New Participant** option.

The *New Participant - General* dialog box opens.
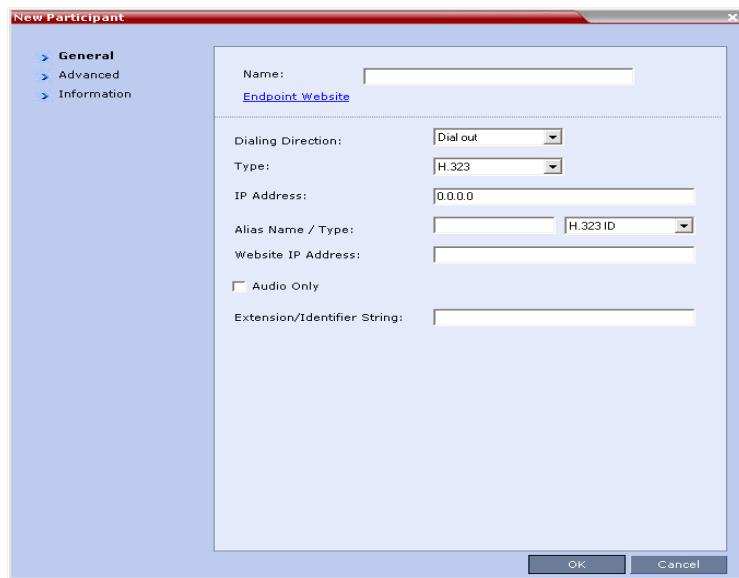
3 Define the following fields:

Table 8-3 *New Participant – General Properties*

Field	Description
Name	Enter the name of the participant or the endpoint as it will be displayed in the Collaboration Server Web Client. The *Name* field can be modified using Unicode encoding. • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. Maximum field length in ASCII is 80 characters. The maximum length of text fields varies according to the mixture of character sets used (Unicode and ASCII). This field may not be left blank. Duplicate participant names, comma, and semi-colon characters may not be used in this field. This name can also become the endpoint name that is displayed in the video layout. For more details about endpoint (site) names, see the *Polycom RMX 1800 Getting Started Guide*, *"Audio and Visual Indications"* on page **3-25**". **Note:** This field is displayed in all tabs.
Endpoint Website	Click the Endpoint Website hyperlink to connect to the internal website of the participant's endpoint. It enables you to perform administrative, configuration and troubleshooting activities on the endpoint. The connection is available only if the IP address of the endpoint's internal site is defined in the *Website IP Address* field.
Dialing Direction	Select the dialing direction: • **Dial-in** – The participant dials in to the conference. This field applies to IP participants only. • **Dial-out** – The MCU dials out to the participant.
Type	The network communication protocol used by the endpoint to connect to the conference: *H.323* or *SIP.* The fields in the dialog box change according to the selected network type.
IP Address	Enter the IP address of the participant's endpoint. • For H.323 participant define either the endpoint IP address or alias. • For SIP participant define either the endpoint IP address or the SIP address.

Table 8-3 New Participant – General Properties (Continued)

Field	Description
Alias Name/Type **(H.323 Only)**	If you are using the endpoint's alias and not the IP address, first select the type of alias and then enter the endpoint's alias: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * and #) • Email ID (email address format, e.g. abc@example.com) • Participant Number (digits 0-9, * and #) **Notes:** • Although all types are supported, the type of alias is dependent on the gatekeeper's capabilities. The most commonly supported alias types are H.323 ID and E.164. • This field is used to enter the Entry Queue ID, target Conference ID and Conference Password when defining a cascaded link. • Use of the E.164 Number is dependent on the setting of the REMOVE_IP_IF_NUMBER_EXISTS System Flag. For more information see "*Substituting E.164 Number in Dial String"* on page **8-13**.
SIP Address/Type **(SIP Only)**	Select the format in which the SIP address is written: • **SIP URI** - Uses the format of an E-mail address, typically containing a user name and a host name: *sip:[user]@[host]*. For example, sip:dan@polycom.com. **Note:** If the *SIP Address* field contains an *IPv6* address, it must be surrounded by square brackets, for example, [::1]. • **TEL URI** - Used when the endpoint does not specify the domain that should interpret a telephone number that has been input by the user. Rather, each domain through which the request passes would be given that opportunity. For example, a user in an airport might log in and send requests through an outbound proxy in the airport. If the users enters "411" (this is the phone number for local directory assistance in the United States), this number needs to be interpreted and processed by the outbound proxy in the airport, and not by the user's home domain. In this case, tel: 411 is the correct choice.
Endpoint Website IP Address	Enter the IP address of the endpoint's internal site to enable connection to it for management and configuration purposes. This field is automatically completed the first time that the endpoint connects to the Collaboration Server. If the field is blank it can be manually completed by the system administrator. The field can be modified while the endpoint is connected
Audio Only	Select this check box to define the participant as a voice participant, with no video capabilities.

Table 8-3 *New Participant – General Properties (Continued)*

Field	Description
Extension/Identifier String	Dial-out participants that connect to an external device such as Cascaded Links or Recording Links may be required to enter a conference password or an identifying string to connect. Enter the required string as follows: **[p]…[p][string]** For example: pp4566# **p** - optional - indicates a pause of one second before sending the **DTMF string**. Enter several concatenated [p]s to increase the delay before sending the string. The required delay depends on the configuration of the external device or conference IVR system. **String** - enter the required string using the digits 0-9 and the characters * and #. The maximum number of characters that can be entered is identical to the H.323 alias length. If the information required to access the device/conference is composed of several strings, for example, the conference ID and the conference password, this information can be entered as one string, where pauses [p] are added between the strings for the required delays, as follows: **[p]…[p][string][p]…[p] [string]...** For example: p23pp*34p4566#
Extension/Identifier String (continued)	The Collaboration Server automatically sends this information upon connection to the destination device/conference. The information is sent by the Collaboration Server as DTMF code to the destination device/conference, simulating the standard IVR procedure.

4   Usually, additional definitions are not required and you can use the system defaults for the remaining parameters. In such a case, click **OK**.

To modify the default settings for advanced parameters, click the **Advanced** tab.

5 Define the following *Advanced* parameters:

Table 8-4 New Participant – Advanced Properties

Field	Description
Video Bit Rate / Auto	The *Auto* check box is automatically selected to use the Line Rate defined for the conference. **Note:** This check box cannot be cleared when defining a new participant during an ongoing conference. To specify the video rate for the endpoint, clear this check box and then select the required video rate.
Video Protocol	Select the video compression standard that will be forced by the MCU on the endpoint when connecting to the conference: *H.261*, *H.263*, *H.264*. Select **Auto** to let the MCU select the video protocol according to the endpoint's capabilities.
Resolution	The *Auto* check box is automatically selected to use the Resolution defined for the conference. To specify the Resolution for the participant, select the required resolution from the drop-down menu.
Encryption	Select whether the endpoint uses encryption for its connection to the conference. **Auto** (default setting) indicates that the endpoint will connect according to the conference encryption setting.

Table 8-4 New Participant – Advanced Properties (Continued)

Field	Description
Cascaded	If this participant is used as a link between conferences select: • **Slave**, if the participant is defined in a conference running on a Slave MCU. • **Master**, if the participant is defined in a conference running on the Master MCU. It enables the connection of one conference directly to another conference using an H.323 connection only. The conferences can run on the same MCU or different MCU's. For more information, see "*Basic Cascading using IP Cascaded Link"* on page **5-3**.
Precedence Domain Name (**Dial-out SIP Only**)	
Precedence Level (**Dial-out SIP Only**)	
AGC	The Audio Gain Control (AGC) protocol that reduces noises is enabled by default for the participants. Clear this check box to disable the AGC feature.

6 To add general information about the participant, such as e-mail, company name, and so on, click the **Information** tab and type the necessary details in the **Info 1-4** fields. Text in the *info* fields can be added in Unicode format (length: 31 characters).

7 Click **OK**.

The new participant is added to the selected group in the address book.

Substituting E.164 Number in Dial String

Between the time a conference is scheduled and when it becomes active, the IP of an endpoint may change, especially in an environment that uses DHCP. The MCU can be set to ignore the IP address of a participant when the conference starts. Instead, the alternative E.164 number will be used.

A new flag, REMOVE_IP_IF_NUMBER_EXISTS, has been added to control this option. This flag must be manually added to change its value. The values of this flag are:

• **YES** (default) - The IP address of an endpoint will be ignored.

• **NO** - The IP address of an endpoint will be used.

Guidelines

• When this feature is enabled, the IP address field of participants in scheduled conferences and conference templates will be empty.

• In order for the MCU to ignore the IP of H.323 participants, the following requirements must be met:
  — A gatekeeper must be defined.
  — The alias of the participant must be defined.
  — The alias type must be defined (not set to *None*).

• If an H.323 gatekeeper is defined but is not connected, the MCU will fail to connect to H.323 dial-out participants.

- In order for the MCU to ignore the IP of SIP participants, the following requirements must be met:
  — A SIP proxy must be defined.
  — The SIP address must be defined.
- If a SIP proxy is defined but is not connected, the MCU will fail to connect to SIP dial-out participants.

Adding a Participant from an Ongoing Conference to the Address Book

You can add a participant to the Address Book directly from an ongoing conference.

> When adding a participant to the address book from a new conference, *Participants* list of an ongoing conference or *Conference Template*, the participant is always added to the "Main" group.

To add a participant from the conference to the Address Book:

1 During an ongoing conference, select the participant in the *Participant* pane and either click the **Add Participant to Address Book** button (▣) or right-click and select **Add Participant to Address Book**.

The participant is added to the Address Book.

Alternatively, you could:

a Double-click the participant's icon or right-click the participant icon and click **Participant Properties**.

The *Participant Properties* window opens.
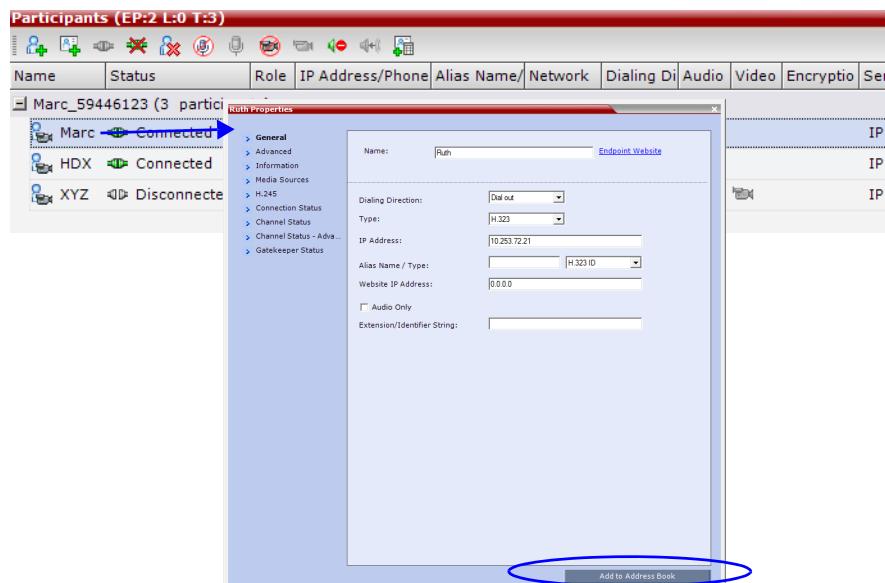
b Click the **Add to Address Book** button.

> If the participant name is already listed in the All Participants list, an error message is displayed. In such a case, change the name of the participant before adding the participant to the address book.

Modifying Participants in the Address Book

When required, you can modify the participant's properties.

To modify participant properties in the Address Book:

1 In the *Address Book - Navigation* pane, select the group to where the participant to modify is listed.

2 In the *Address Book - List* pane, double-click the participant's icon. The *Participant's Properties* window is displayed.
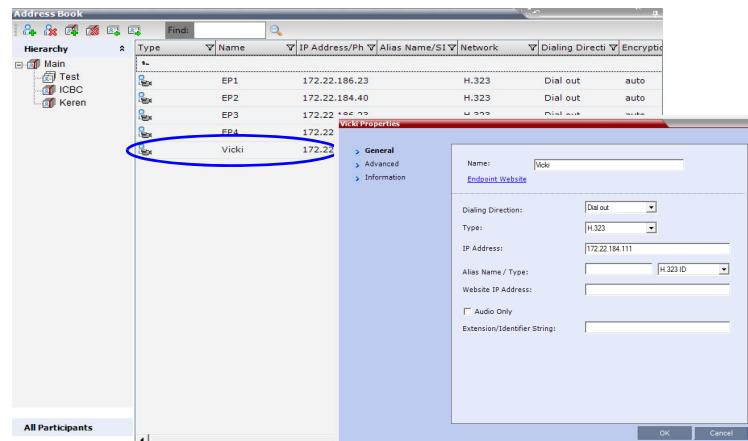
3 Modify the necessary properties in the window, such as dialing direction, communication protocol type, and so on. You can modify any property in any of the three tabs: *General*, *Advanced* and *Info*.

4 Click **OK**.

The changes to the participant's properties are updated.

Deleting Participants from the Address Book

To delete participants from the Address Book:

1 In the *Address Book - Navigation* pane, select the group where the participant to delete is listed.

2 In the *Address Book - List* pane, either select the participant to delete and then click the **Delete Participant** (⊠) button, or right-click the participant icon and then click the **Delete Participant** option.
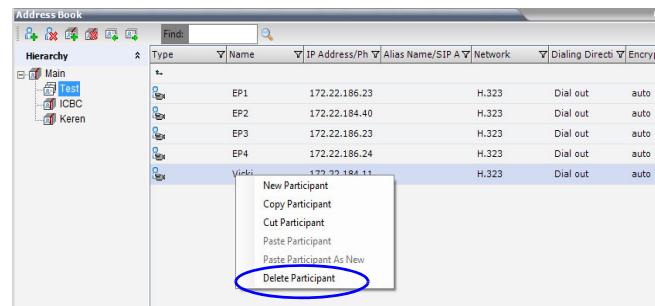
3 A confirmation message is displayed depending on the participant's assignment to groups in the address book:

a When the participant belongs to only one group: click **Yes** to permanently delete the participant from the address book.

b When the participant belongs to multiple groups, a message is displayed requesting whether to delete the participant from the *Address Book* or from the current selected group. Select:

- **Current group** to delete the participant from the selected group
- **Address Book** to permanently delete the participant from the address book (all groups).

Click **OK** to perform the delete operation or **Cancel** to exit the delete operation.

Copying or Moving a Participant

You can copy or move a participant from one group to another group using the **Copy**, **Cut**, and **Paste** options. A participant can belong to multiple groups. However, there is only one entity per participant. Groups that contain the same participants refer to the same definition of the participant entity. Alternatively, you can drag a participant from one location in the *Address Book* to another location, moving the participant to its new location using the drag-and-drop operation.

> The cut and copy actions are not available when selecting multiple participants.

To copy or move a participant to another group:

1 In the *Address Book - Navigation* pane, select the group from where to copy the participant.

2 In the *Address Book - List* pane, select the participant you want to copy.

3 Right-click the selected participant and select one of the following functions from the drop-down menu:
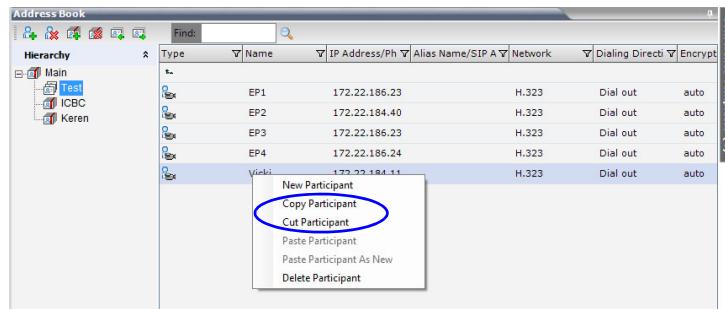
Table 8-5   *Copy/Cut Functions*

Function	Description
Copy Participant	Copies the participant to be pasted into an additional group.
Cut Participant	Moves the participant from the current group to a different group. Alternatively, you can move a participant to another location by dragging the participant to the new location.

4 In the *Address Book* navigation pane, navigate and select the group in which you want to paste the participant.

5 Right-click the selected group and click one of the following **Paste** functions from the drop-down menu:

Table 8-6   Paste functions

Function	Description
Paste Participant	Creates a link to the participant entity in the pasted location.
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds "*Copy*" to the end of the participant name.

The Paste functions are only available after a **Copy** or **Cut** action has been implemented.

To drag a participant from an address book group to another group:

1 Select the participant or participants you want to move.

2 Click and hold the left mouse button and drag the selection to the new group.

The participants are moved to the new address book group.

Searching the Address Book

You can search the *Address Book* for a participant's name or a group name only on the currently selected group/level.

To search for participants or groups in the current selected level:

1 In the *Address Book Navigation* pane, select the group/level within to run the search.

2 In the *Address Book* toolbar, activate the search option by clicking the **Find** field.

The field clears and a cursor appears indicating that the field is active.

3 Type all or part of the participant's name or group name and click the search button.

The closest matching participant entries are displayed and the Active Filter indicator turns on.

Filtering the Address Book

The entries in an address book group can be filtered to display only the entries (participants or groups) that meet criteria that you specify and hides entries that you do not want displayed. It enables you to select and work with a subset of *Address Book* entries.

You can filter by more than one column, by adding additional filters (columns).

The filter applies to the displayed group. If *All Participants* option is selected, it applies to all the listed participants.

Filtering can be done using:

- A predefined pattern
- Customized pattern

When you use the Find dialog box to search filtered data, only the data that is displayed is searched; data that is not displayed is not searched. To search all the data, clear all filters.

Filtering Address Book Data Using a Predefined Pattern

To filter the data in an address book group:

1 In the *Address Book - Navigation* pane, select the group to filter.

2 In the *Address Book - List* pane, in the *column* that you want to use for filtering, click the filter (▽) button.

A drop-down menu is displayed containing all the matching patterns that can be applied to the selected field.
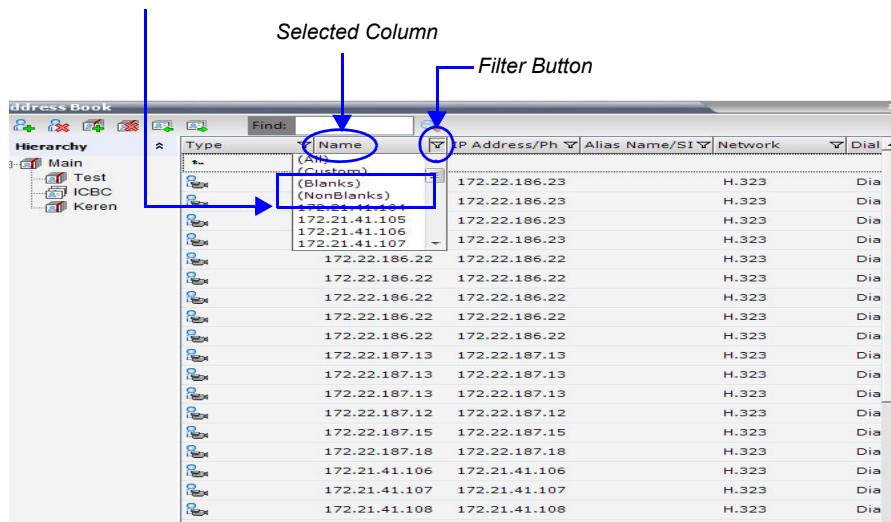
3 Click the matching pattern to be applied.

The filtered list is displayed with a filter indicator (▼) displayed in the selected column heading.

Example: If the user selects **172.21.41.104** as the matching pattern, the filtered group in the *Address Book* is displayed as follows:
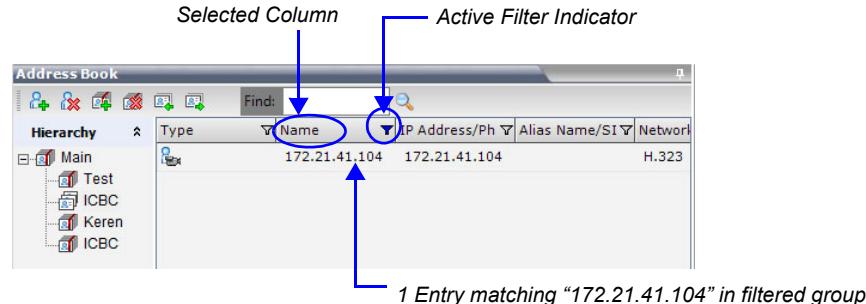
Filtering Address Book Data Using a Custom Pattern

To filter the data in an address book group:

1 In the *Address Book - Navigation* pane, select the group to filter.

2 In the *Address Book - List* pane, in the *column* that you want to use for filtering, click the filter (▽) button.

3 Select the **(Custom)** option from the drop-down list.
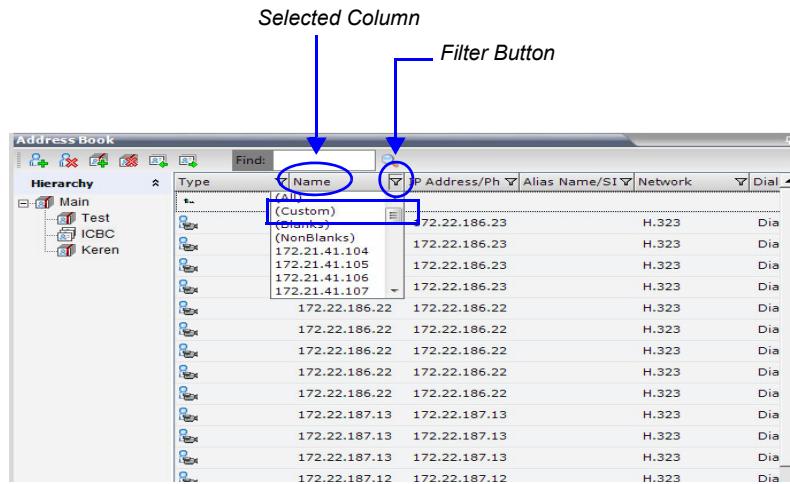
The *Custom Filtering* dialog box opens.
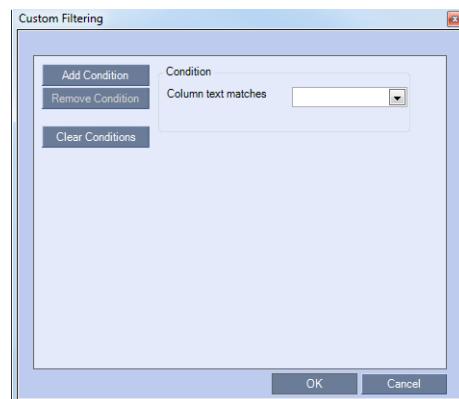
4 In the *Condition - Column text matches* field, enter the filtering pattern.
For example, to list only endpoints that include the numerals 41 in their name, enter 41.

5 **Optional.** Click the **Add Condition** button to define additional filtering patterns to further filter the list and fine tune your search.

To clear a filtering pattern, click the **Clear Condition** button.

The filtered list is displayed with an active filter (blue) indicator (▼) displayed in the selected column heading. For example, if the filtering pattern is 41, the participants list includes all the endpoints that contain the numerals 41 in their name.

Clearing the Filter

To clear the filter and display all entries:

1 In the filtered *Address Book* column heading, click the *Active Filter* indicator.

The pattern matching options menu is displayed.

2 Click (**All**).

The filter is deactivated and all the *group/level* entries are displayed.

Obtaining the Display Name from the Address Book

The MCU can be configured to replace the name of the dial-in participant as defined in the endpoint (site name) with the name defined in the Address Book.

In this process, the system retrieves the data (name, alias, number or IP address) of the dial-in participant and compares it first with the conference defined dial-in participants and if the endpoint is not found, it then searches for the endpoint with entries in the address book. After a match is found, the system displays the participant name as defined in the address book instead of the site name, in both the video layout and the Collaboration Server Web Client/Manager.

The system compares the following endpoint data with the address book entries:

- For H.323 participants, the system compares the IP address, Alias, or H.323 number.
- For SIP participants, the system compares the IP address or the SIP URI.

Guidelines

Guidelines

- Only Users with *Administrator* and *Operator* Authorization Levels are allowed to enable and disable the *Obtain Display Name from Address Book* feature.
- This feature is supported only for IPv4 participants.

Enabling and Disabling the Obtain Display Name from Address Book Feature

Enabling and Disabling the Obtain Display Name from Address Book Feature

The *Obtain Display Name from Address Book* option can be enabled for all participants connecting to the MCU if the name of the participants are defined in the Address Book.

To enable or disable the Obtain Display Name from Address Book option:

1   On the Collaboration Server main menu bar, click **Setup > Customize Display Settings > Ongoing Conferences**.

The *Ongoing Conferences* dialog box is displayed.
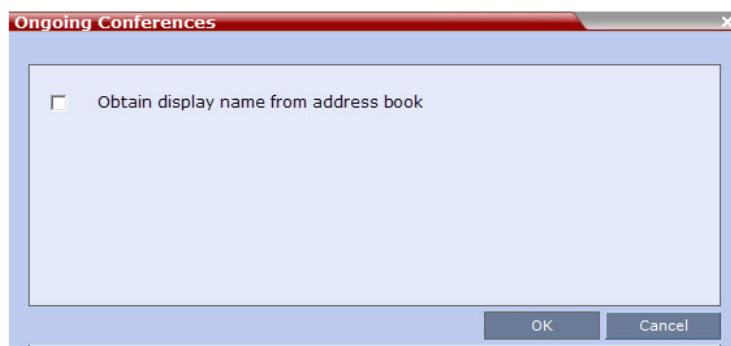
2   Select the **Obtain display name from address book** check box to enable the feature or clear the check box to disable the feature.

3 Click **OK**.

Importing and Exporting Address Books

Address Books are proprietary Polycom data files that can only be distributed among Collaboration Server units. The Address Books are exported in XML format, which are editable offline. If no name is assigned to the exported Address Book, the default file name is: `EMA.DataObjects.OfflineTemplates.AddressbookContent_.xml`

Exporting an Address Book

To Export an Address Book:

1 In the *Address Book* pane, click the **Export Address Book** (⊞) button or right-click an empty area in the pane and click **Export Address Book**.

The *Export Address Book* dialog box is displayed.
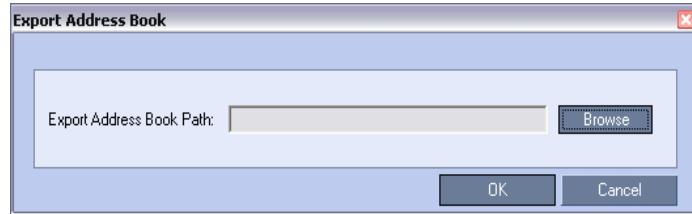
2 Enter the desired path or click the **Browse** button.

3 In the **Save Address Book** dialog box, select the directory to save the file. You may also rename the file in the *File Name* field.

4 Click **Save**.
You will return to the *Export File* dialog box.

5 Click **OK**.
The exported Address Book is saved in the selected folder in XML format.

Importing an Address Book

To Import and Address Book:

1 In the *Address Book* pane, click the **Import Address Book** (⊞) button or right-click an empty area in the pane and then click **Import Address Book**.

The *Import Address Book* dialog box is displayed.
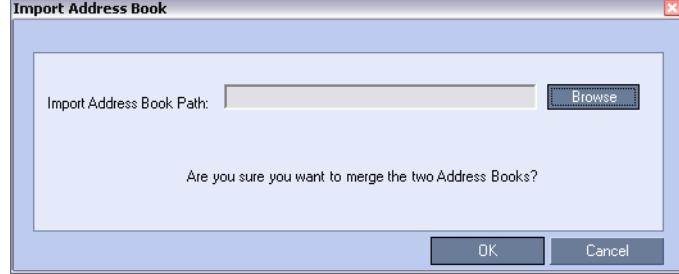
2 Enter the path from which to import the Address Book or click the **Browse** button.

3 In the *Open* dialog box navigate to the desired Address Book file (in XML format) to import.

When importing an Address Book, participants with exact names in the current Address Book will be overwritten by participants defined in the imported Address Book.

4   Click **Open**.

You will return to the *Import File* dialog box.

5   Click **OK**.

The *Address Book* is imported and a confirmation message is displayed at the end of the process.

6   Click Close.

9

Reservations

The *Reservations* option enables users to schedule conferences. These conferences can be launched immediately or become ongoing, at a specified time on a specified date.

Scheduling a conference reservation requires definition of conference parameters such as the date and time at which the conference is to start, the participants and the duration of the conference.

Scheduled conferences (Reservations) can occur once or repeatedly, and the recurrence pattern can vary.

The maximum number of reservations per Collaboration Server is 2000.

Guidelines

Resources

Maximum number of participants (voice and video) in a CP reservation:

- Polycom RMX 1800 with 3 video accelerators: Up to 100 HD 720p 30 or 50 HD 1080p 25/30 fps.
- Polycom RMX 1800 with 2 video accelerators: Up to 70 HD 720p 30 or 35 HD 1080p 25/30 fps.
- Polycom RMX 1800 with 1 video accelerators: Up to 100 HD 720p 35 or 17 HD 1080p 25/30 fps.
- System resources are calculated according to the Collaboration Server's license. For more information see "*Forcing Video Resource Allocation to CIF Resolution*" on page **19-6**.
- System resource availability is partially checked when reservations are created:
    - If a conference duration extension request is received from an ongoing conference, the request is rejected if it would cause a resource conflict.
    - If several reservations are scheduled to be activated at the same time and there are not enough resources for all participants to be connected:
        - The conferences are activated.
        - Participants are connected to all the ongoing conferences until all system resources are used up.
- If sufficient resources are not available in the system and a scheduled *Reservation* cannot be activated, the *Reservation* is deleted from the schedule.
- Resources are reserved for participants at the highest video resolution supported by the *Line Rate* specified in the conference *Profile* and up to the maximum system video resolution specified by the *Resolution Configuration* dialog box.

- When a new *Reservation* is created in the *Reservation Calendar*, the effect of the new *Reservation* (including its recurrences) on available resources is checked. If resource deficiencies are found an error message is displayed.

  Defined dial-in or dial-out participants, Meeting Rooms, Entry Queues and new connections to Ongoing conferences are not included in the resources calculation.

Reservations

- A *Reservation* that has been activated and becomes an ongoing conference is deleted from the *Reservation Calendar* list.
- The maximum number of concurrent reservations is 80. Reservations with durations that overlap (for any amount of time) are considered to be concurrent.
- System resource availability is partially checked when reservations are created:
  — If a conference duration extension request is received from an ongoing conference, the request is rejected if it would cause a resource conflict.
  — If several reservations are scheduled to be activated at the same time and there are not enough resources for all participants to be connected:
    - The conferences are activated.
    - Participants are connected to all the ongoing conferences until all system resources are used up.
- A scheduled *Reservation* cannot be activated and is deleted from the schedule if:
  — An Ongoing conference has the same *Numeric ID*.
  — Sufficient resources are not available in the system.
- If a problem prevents a *Reservation* from being activated at its schedule time, the *Reservation* will not be activated at all. This applies even if the problem is resolved during the *Reservation's* scheduled time slot.
- A Profile that is assigned to a Reservation cannot be deleted.
- Reservations are backed up and restored during **Setup > Software Management >Backup /Restore Configuration** operations. For more information see "*Software Management*" on page **19-37**.
- All existing reservations are erased by the *Standard Restore* option of the **Administration > Tools > Restore Factory Defaults** procedure.
- *Reservations* can also be scheduled from *Conference Templates*. For more information see see "*Scheduling a Reservation From a Conference Template*" on page **11-9**.

Using the Reservation Calendar

To open the Reservation Calendar:

>> In the *RMX Management* pane, click the *Reservation Calendar* button (▦).
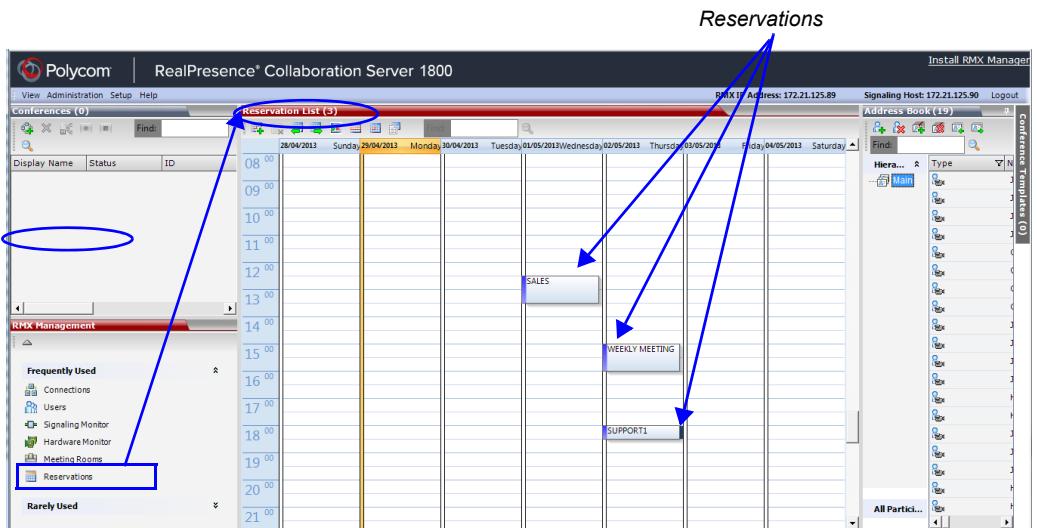
Reservations

Toolbar Buttons

The toolbar buttons functions are described in Table 9-1.

Table 9-1 Reservations – Toolbar

Button	Description
New Reservation	Create a new reservation. The date and time of the new reservation is set according to the highlighted blocks on the *Reservation Calendar*.
Delete Reservation	Click to delete the selected reservation.
Back	Click to show the previous day or week, depending on whether *Show Day* or *Show Week* is the selected.
Next	Click to show the next day or week, depending on whether *Show Day* or *Show Week* is the selected.
Today	Click to show the current date in the Reservation Calendar in either *Show Day* or *Show Week* view.
Show Week	Change the calendar view to weekly display, showing a calendar week: Sunday through Saturday
Show Day	Click this button to show the day containing the selected time slot.
Reservations List	Click to change to List View and display a list of all reservations.
Find:	Used to search for reservations by *Display Name.* (Available in *Reservations List view* only).

Reservations Views

The *Reservation Calendar* list has the following views available:

*   Week
*   Day
*   Today
*   List

In all views the *Main Window List Pane* header displays the total number of reservations in the system.

Total number of reservations

Week View

By default the *Reservation Calendar* is displayed in *Week* view with the current date highlighted in orange.
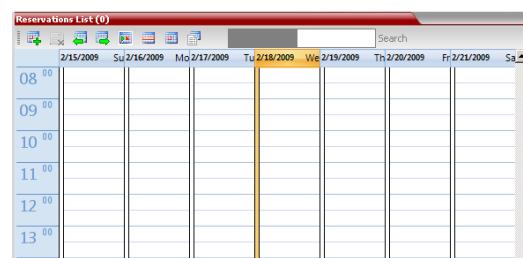
Day View

A single day is displayed.

Today View

The current date (*Today*), highlighted in orange, can be viewed in both *Week View* and *Day View*.

Current Date (Today)
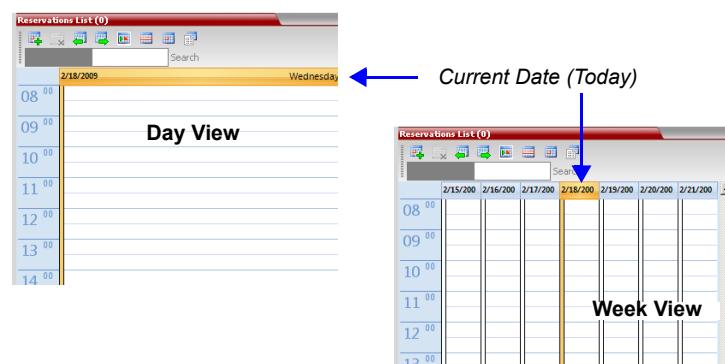
List View

List View does not have a calendar based format.

All *Reservations* are listed by:

- *Display Name*
- *ID*
- *Internal ID*
- *Start Time*

- *End Time*
- *Status*
- *Conference Password*
- *Profile*

The *Reservations* can be sorted, searched and browsed by any of the listed fields.

Changing the Calendar View

To change between Week and Day views:

>> In Week View: In the *Reservation Calendar* toolbar, click **Show Day** ( ) to change to *Day View*.

or

In Day View: In the *Reservation Calendar* toolbar, click **Show Week** ( ) to change to *Week View*.

Week View

Back – *View Previous Week*
Next – *View Next Week*
Today – *View Current Date in Week View*

Current Date

Show Day   *Show Week*

Day View

Back – *View Previous Day*
Next – *View Next Day*
Today – *View Current Date in Day View*
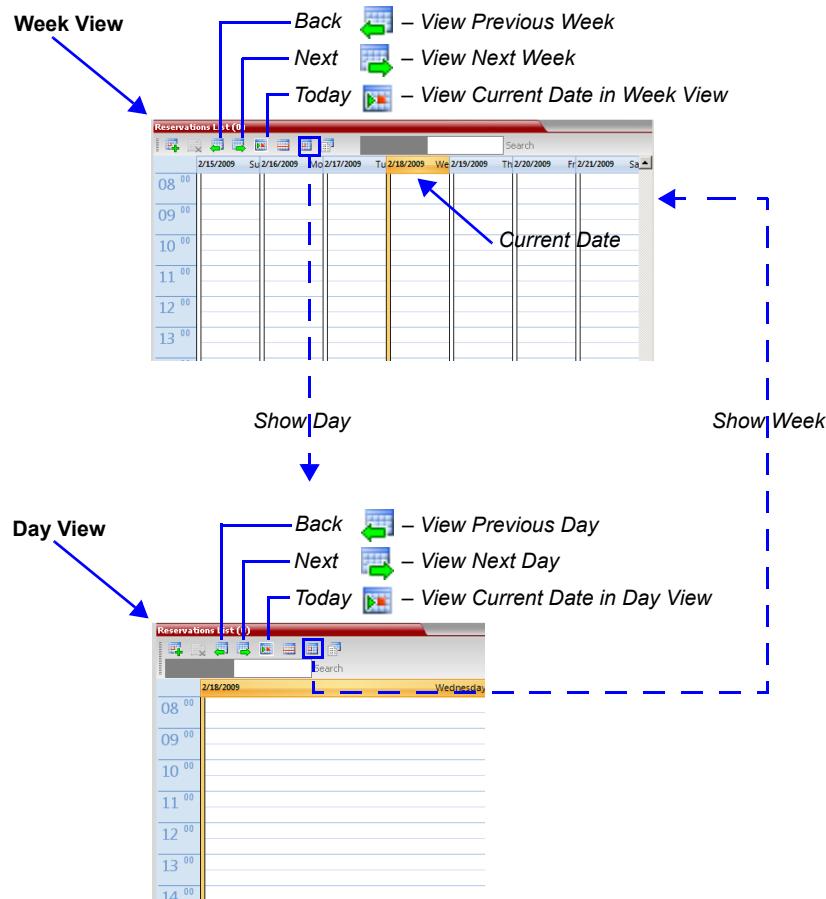
To view Today (the current date):

>> In *Week View* or *Day View*, in the *Reservation Calendar* toolbar, click the **Today** (![icon])
button to have the current date displayed within the selected view.

Week View
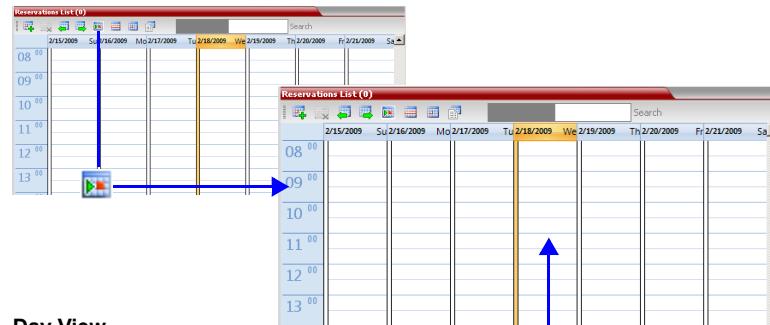
Day View
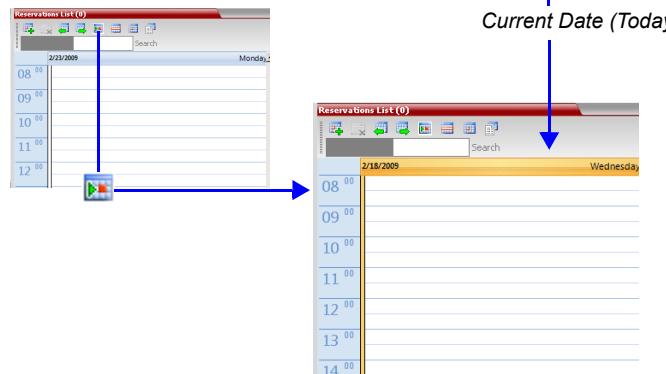
Current Date (Today)

To change to List View:

1 In the *Reservation Calendar* toolbar, click, the **Reservations List** (![icon]) button.

The *Reservations List* is displayed.

Display Name	ID	Start Time	End Time	Internal ID	Status	Conference Passw	Profile
SUPPORT_180	17989	07/11/2008 05:00	07/11/2008 05:30	183	ok	987654	Factory_Video_Profile
SUPPORT_157	91272	06/11/2008 18:30	06/11/2008 19:30	169	ok		Factory_Video_Profile
SUPPORT_108	97493	06/11/2008 18:30	06/11/2008 19:30	170	ok		Factory_Video_Profile
Logistics	00582	05/11/2008 15:00	05/11/2008 17:00	168	ok		Factory_Video_Profile
Sales	12295	04/11/2008 12:00	04/11/2008 13:00	167	ok		Factory_Video_Profile
deb_template1	20940	02/11/2008 23:45	03/11/2008 00:45	127	ok		Factory_Video_Profile

2 **Optional.** Sort the data by any field (column heading) by clicking on the column
heading.

A ▽ or △ symbol is displayed in the column heading indicating that the list is sorted
by this field, as well as the sort order.

3 **Optional.** Click on the column heading to toggle the column's sort order.

To return to Calendar View:

>> In the *Reservation Calendar* toolbar, click any of the buttons (**Show Week/Show Day/
Today**) to return to the required *Reservation Calendar* view.

Scheduling Conferences Using the Reservation Calendar

Creating a New Reservation

There are three methods of creating a new reservation:

*   Method I – Creating a reservation with default duration of 1 hour
*   Method II – Creating a reservation with default duration of ½ hour
*   Method III – Interactively define the reservation duration

Each method requires the selection of a starting time slot in the *Reservation Calendar*. The default time slot is the current half-hour period of local time.

In all views, if the **New Reservation** ( ) button is clicked without selecting a starting time slot or if a time slot is selected that is in the past, the *Reservation* becomes an Ongoing conference immediately and is not added to the *Reservations* calendar.
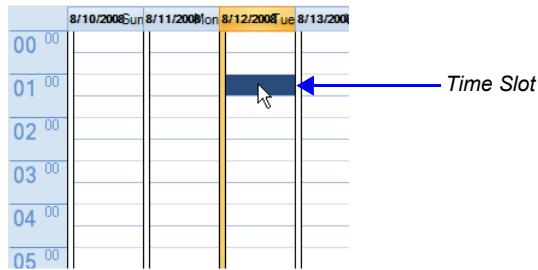
After selecting a starting time slot in the *Reservation Calendar* you can create a reservation with a default duration derived from the creation method used or by interactively defining the duration of the reservation.

Method I – To create a reservation with default duration of 1 hour:

>>   In the *Reservation Calendar* toolbar, click the **New Reservation** ( ) button to create a reservation of 1 hour duration.

Method II – To create a reservation with default duration of ½ hour:

>>   Right-click and select **New Reservation** to create a reservation of ½ hour default duration.

Method III – To interactively define the duration:

1   In the calendar, click & drag to expand the time slot to select the required *Date*, *Start Time and Duration* for the reservation.

2   In the *Reservation Calendar* toolbar, click the **New Reservation** ( ) button or right-click and select **New Reservation.**

Example: The following click & drag sequence would select a reservation for *Tuesday, August 12, 2008*, starting at *01:00* with a duration of *4* hours.
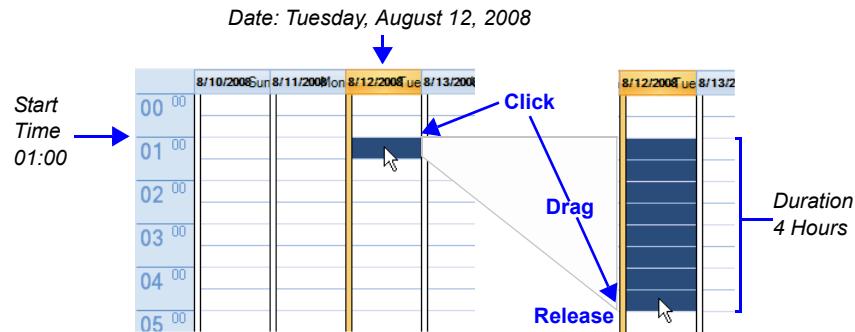
The duration of reservations created by any of the above methods can be modified in the *Scheduler* tab of the *New Reservation* dialog box.

To create a new reservation:

1 Open the *Reservation Calendar*.

2 Select a starting time slot.

3 Create the reservation using one of the three methods described above.

The *New Reservation – General* tab dialog box opens.
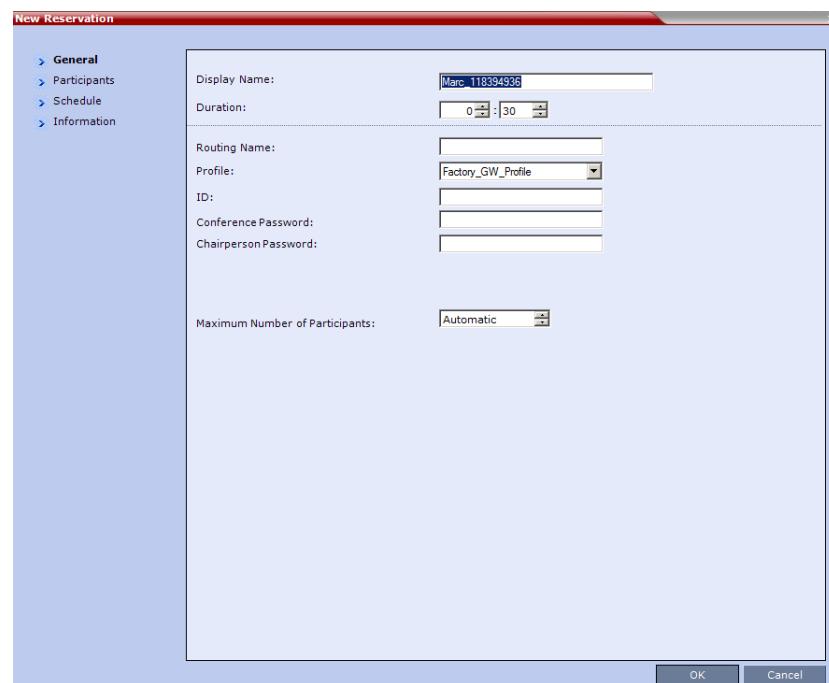
All the fields are the same as for the *New Conference – General* tab, described in the *Polycom RMX 1800 Getting Started Guide*, *"General Tab"* on page **3-14**.

> When a *Conference Profile* is assigned to a Meeting Room or a Reservation, the Profile's parameters are not embedded in the Reservation, and are taken from the Profile when the reservation becomes an ongoing conference. Therefore, any changes to the Profile parameters between the time the Reservation or Meeting Room was created and the time that it is activated (and becomes an ongoing conference) will be applied to the conference.
> If the user wants to save the current parameters, a different Profile with these parameters must be assigned, or a different Profile with the new parameters must be created.

4 Click the **Schedule** tab.

Calendar
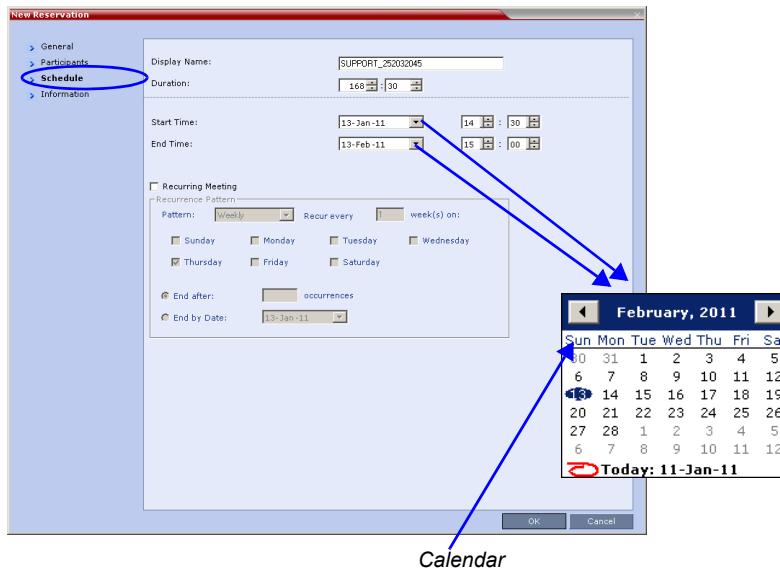
5 Adjust the new reservation's schedule by modifying the fields as described in Table 9-2.

Table 9-2   *New Reservation – Schedule Tab*

Field	Description	
Start Time	Select the Start Time of the Reservation.	• The Start/End Times of the Reservation are initially taken from the time slot selected in the Reservation Calendar. • The Start/End Times can be adjusted by typing in the hours and minutes fields or by clicking the arrow buttons. • The Start/End dates can be adjusted by typing in the date field or by clicking the arrow buttons or using the calendar. • The start time of all the reservations can be manually adjusted in one operation. For more information see "*Adjusting the Start Times of all Reservations"* on page **9-16**.
End Time	Select the End Time of the Reservation.	• End Time settings are initially calculated as Start Time + Duration. End Time settings are recalculated if Start Time settings are changed. • Changes to End Time settings do not affect Start Time settings. However, the Duration of the Reservation is recalculated.
Recurring Meeting	Select this option to set up a Recurring Reservation - a series of Reservations to be repeated on a regular basis. To create a recurring reservation, you must define a time period and a recurrence pattern of how often the Reservation should occur: *Daily*, *Weekly* or *Monthly*.	

Table 9-2   *New Reservation – Schedule Tab (Continued)*

Field	Description	
Recurrence Pattern	Daily	If *Daily* is selected, the system automatically selects all the days of the week. To de-select days (for example, weekends) clear their check boxes.
	Weekly	If *Weekly* is selected, the system automatically selects the day of the week for the Reservation from the day selected in the Reservation Calendar. You can also define the recurrence interval in weeks. For example, if you want the reservation to occur every second week, enter 2 in the *Recur every _ week(s)* field. To define a twice-weekly recurring Reservation, select the check box of the additional day of the week on which the Reservation is to be scheduled and set the recurrence interval to 1.
	Monthly	If *Monthly* is selected, the system automatically selects the day of the month as selected in the Reservation Calendar. You are required to choose a recurrence pattern: • **Day (1-31) of every (1-12) month(s**) - Repeats a conference on a specified day of the month at a specified monthly interval. For example, if the first Reservation is scheduled for the 6th day of the current month and the monthly interval is set to 1, the monthly Reservation will occur on the 6th day of each of the following months. • **The (first, second,...,last) (Sun-Sat) of x month(s)** - Repeats a Reservation in a particular week, on a specified day of the week at the specified monthly interval. For example, a recurrent meeting on the third Monday every second month.
A series of Reservations can be set to end after a specified number of occurrences or by a specific date. Select one of the following methods of terminating the series of Reservations:		
End After	**End After: x Occurrences** - Ends a recurring series of Reservations after a specific number (x) of occurrences. Default: 1 (Leaving the field blank defaults to 1 occurrence.)	
End by Date	**End By Date: mm/dd/yyyy** - Specifies a date for the last occurrence of the recurring series of Reservations. The End By Date value can be adjusted by typing in the date field or by clicking the arrow button and using the calendar utility. Default: Current date.	

6 Click the **Participants** tab.

The fields are the same as for the *New Conference – Participants* tab, described in the *Polycom RMX 1800 Getting Started Guide*, "*Participants Tab*" on page **3-16**.

Participant properties are embedded in the conferencing entity and therefore, if the participant properties are modified in the *Address Book* (or *Meeting Rooms*) after the Reservation has been created they are not applied to the participant when the Reservation is activated.

7 **Optional.** Add participants from the *Participants Address Book*.

For more information see "*Meeting Rooms*" on page **6-1** and the *Polycom RMX 1800 Getting Started Guidee*, "*To add participants from the Address Book:*" on page **3-18**.

Between the time a conference is scheduled and when it becomes active, the IP of an endpoint may change, especially in an environment that uses DHCP. The MCU can be set to ignore the IP address of a participant when the conference starts. Instead, the alternative E.164 number will be used instead of the IP address. For more information see "*Substituting E.164 Number in Dial String*" on page **8-13**.

8 **Optional.** Add information to the reservation.

Information entered in the *Information* tab is written to the *Call Detail Record (CDR)* when the reservation is activated. Changes made to this information before it becomes an ongoing conference will be saved to the CDR.

For more information see the *Polycom RMX 1800 Getting Started Guide*, "*Information Tab*" on page **3-18**.

9 Click **OK**.
The *New Reservation* is created and is displayed in the *Reservation Calendar*.

If you create a recurring reservation all occurrences have the same ID. The series number (_0000n) of each reservation is appended to its *Display Name*.

Example:

Conference Template name: `Sales`

Display Name for single scheduled occurrence: `Sales`

If 3 recurrences of the reservation are created:

Display Name for occurrence 1:   `Sales_00001`

Display Name for occurrence 2:   `Sales_00002`

Display Name for occurrence 3:   `Sales_00003`

Managing Reservations

Reservations can be accessed and managed via all the views of the *Reservations List*.

Guidelines

* The *Recurrence Pattern* fields in the *Schedule* tab that are used to create multiple occurrences of a *Reservation* are only displayed when the *Reservation* and its multiple occurrences are initially created.
* As with single occurrence *Reservations*, only the *Duration*, *Start Time* and *End Time* parameters of multiple occurrence reservations can be modified after the *Reservation* has been created.
* A single occurrence *Reservation* cannot be modified to become a multiple occurrence reservation.
* *Reservations* can only be modified one at a time and not as a group.
* If *Reservations* were created as a recurring series, the system gives the option to delete them individually, or all as series.

Viewing and Modifying Reservations

Reservations can be viewed and modified by using the *Week* and *Day* views of the *Reservations Calendar* or by using the *Reservation Properties* dialog box.

Using the Week and Day views of the Reservations Calendar

In the *Week* and *Day* views each *Reservation* is represented by a shaded square on the *Reservation Calendar*. Clicking on a *Reservation* selects the *Reservation*. A dark blue border is displayed around the edges of the *Reservation* indicating that it has been selected.

The *Start Time* of the *Reservation* is represented by the top edge of the square while the *End Time* is represented by the bottom edge.

The cursor changes to a vertical double arrow (↕) when it is moved over the top and bottom sides of the square.
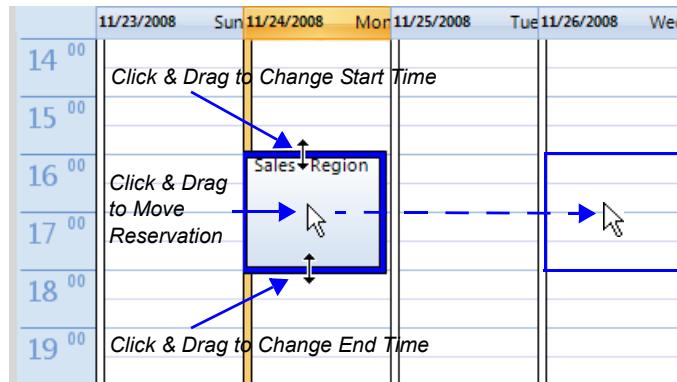
To move the Reservation to another time slot:

1 Select the *Reservation*.

2 Hold the mouse button down and drag the *Reservation* to the desired time slot.

3 Release the mouse button.

To change the Reservation's Start time:

1 Select the *Reservation*.

2 Move the mouse over the top edge of the *Reservation's* square.

3 When the cursor changes to a vertical double arrow (↕) hold the mouse button down and drag the edge to the desired *Start Time.*

4 Release the mouse button.

To change the Reservation's End time:

1 Select the *Reservation*.

2 Move the mouse over the bottom edge of the *Reservation's* square.

3 When the cursor changes to a vertical double arrow (↕) hold the mouse button down and drag the edge to the desired *End Time.*

4 Release the mouse button.

To View or Modify Reservations using the Reservation Properties dialog box:

1 In the *Reservations List*, navigate to the reservation (or its recurrences) you want to view, using the **Show Day**, **Show Week**, **Today**, **Back**, **Next** or **List** buttons.

2 Double-click, or right-click and select **Reservation Properties**, to select the reservation to be viewed or modified.

The *Reservation Properties – General* dialog box opens.

3 Select the tab(s) of the properties you want to view or modify.

4 **Optional.** Modify the *Reservation Properties*.

5 Click **OK**.
The dialog box closes and modifications (if any) are saved.

Adjusting the Start Times of all Reservations

When utilizing GMT offset (for example, *Daylight Saving Time* change), the start time of the reoccurring reservations scheduled before the Collaboration Server time change are not updated accordingly (although their start times appear correctly in the *Reservations* list, when checking the reservation properties the start time is incorrect).

Following the Collaboration Server time change, the start time of all reoccurring reservations must be manually adjusted in one operation.

Using this option, the start times of **all** reservations currently scheduled on the Collaboration Server are adjusted with the same offset.

To adjust the reoccurring reservations start time after the GMT Offset has been changed for Daylight Saving Time (DST) or a physical move:.

> Adjustment of *Reservation Time* should only be performed after adjustment of *Collaboration Server Time* is completed as a separate procedure.

1 On the Collaboration Server menu, click **Setup > RMX Time**.
The *RMX Time* dialog box opens.

2 Click the **Adjust Reservations Time** button.
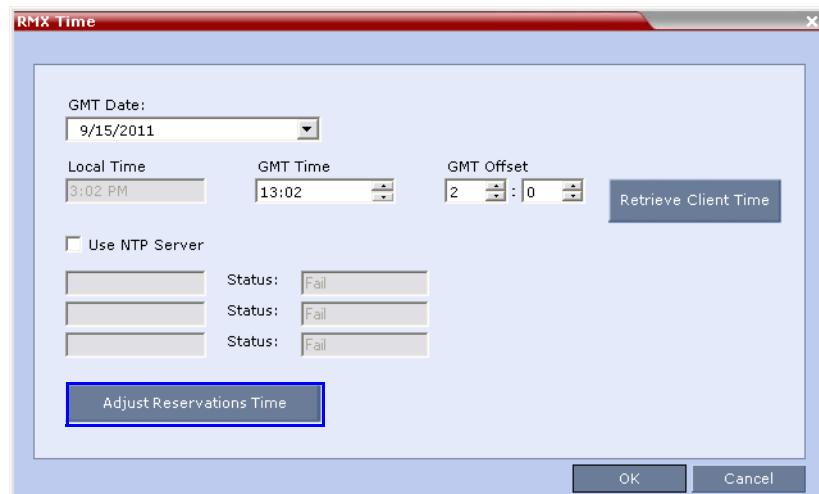
The *Adjust Reservations Time* dialog box opens.
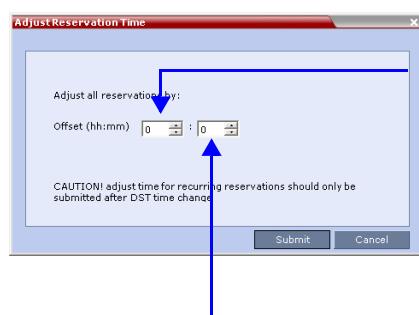
*Click the arrows to adjust the start time by hours.
Range is between 12 hours and -12 hours
A positive value indicates adding to the start time
(-) indicates subtracting from the start time*

*Click the arrows to adjust the start time by minutes.
Range is between 45 minutes and -45 minutes.
A positive value indicates adding to the start time
(-) indicates subtracting from the start time*

3 Click the arrows of the *Offset - Hours* box to indicate the number of hours to add or subtract from the current start time; a positive value indicates adding time, while minus (-) indicates subtracting time.

4 Click the arrows of the *Offset - minutes* box to indicate the number of minutes to add or subtract from the current start time of the reservations. Increments or decrements are by 15 minutes.

For example, to subtract 30 minutes from the start time of all the reservation, enter 0 in the *hours* box, and -30 in the *minutes* box.

To add one hour and 30 minutes to the start time, enter 1 in the hours box and 30 in the minutes box.

5 Click the **Adjust** button to apply the change to all the reoccurring reservations currently scheduled on the Collaboration Server.

> When adjusting the start time of 1000 - 2000 reservations, an "Internal communication error" message may appear. Ignore this message as the process completes successfully.

Deleting Reservations

To delete a single reservation:

1 In the *Reservations List*, navigate to the reservation you want to delete, using the **Show Day**, **Show Week**, **Today**, **Back**, **Next** or **List** buttons.

2 Click to select the reservation to be deleted.

3 Click the **Delete Reservation** (✖) button.
or
Place the mouse pointer within the *Reservation* block, right-click and select **Delete Reservation**.

4 Click **OK** in the confirmation dialog box.
The *Reservation* is deleted.

To delete all recurrences of a reservation:

1 In the *Reservations List*, navigate to the *Reservation* or any of its recurrences, using the **Show Day**, **Show Week**, **Today**, **Back**, **Next** or **List** buttons.

2 Click the **Delete Reservation** (✖) button.
or
Place the mouse pointer within the *Reservation* or any of its recurrences, right-click and select **Delete Reservation**.

A confirmation dialog box is displayed.

3 Select **Delete the series.**

4 Click **OK.**

All occurrences of the *Reservation* are deleted.

Searching for Reservations using Quick Search

Quick Search is available only in *List View*. It enables you to search for *Reservations* by *Display Name*.

To search for reservations:

1 In the *Reservation Calendar* toolbar, click in the *Quick Search* field.

The field clears and a cursor is displayed indicating that the field is active.

| Find: | 🔍 | ➜ | Find: | | 🔍 |

2 Type all or part of the reservation's *Display Name* into the field and click **Search**.

The closest matching *Reservation* entries are displayed.

Display Name	ID	Start Time	End Time	Internal ID	Status	Conference Pass	Chairperson Pas	Profile
Sales 1	57162	27/11/2008	27/11/20	150	ok			Factory_Vid
Sales 1	57162	25/11/2008	25/11/20	148	ok			Factory_Vid
Sales 2	57168	24/11/2008	24/11/20	147	ok			Factory_Vid
Sales 2	57168	26/11/2008	26/11/20	149	ok			Factory_Vid
Sales 0	57162	28/11/2008	28/11/20	151	ok			Factory_Vid

Closest Matching Reservations

3 **Optional.** Double- click the *Reservation's* entry in the list to open the *Reservations Properties* dialog box to view or modify the *Reservation*.

or

Right -click the *Reservation's* entry in the list and select a menu option to view, modify or delete the *Reservation*.

To clear the search and display all reservations:

1 Clear the *Quick Search* field.

2 Click **Search.**

All *Reservations* are displayed.

10

Operator Assistance & Participant Move

Users (operators) assistance to participants is available when:

- Participants have requested individual help (using *0 DTMF code) during the conference.
- Participants have requested help for the conference (using 00 DTMF code) during the conference.
- Participants have problems connecting to conferences, for example, when they enter the wrong conference ID or password.

In addition, the user (operator) can join the ongoing conference and assist all conference participants.

Operator assistance is available only when an *Operator conference* is running on the MCU.

The *Operator conference* offers additional conference management capabilities to the Collaboration Server users, enabling them to attend to participants with special requirements and acquire participant details for billing and statistics. This service is designed usually for large conferences that require the personal touch.

Operator Conferences

An *Operator conference* is a special conference that enables the Collaboration Server user acting as an operator to assist participants without disturbing the ongoing conferences and without being heard by other conference participants. The operator can move a participant from the Entry Queue or ongoing conference to a private, one-on-one conversation in the Operator conference.

In attended mode, the Collaboration Server user (operator) can perform one of the following actions:

- Participants connected to the Entry Queue who fail to enter the correct destination ID or conference password can be moved by the user to the Operator conference for assistance.
- After a short conversation, the operator can move the participant from the Operator conference to the appropriate destination conference (Home conference).
- The operator can connect participants belonging to the same destination conference to their conference simultaneously by selecting the appropriate participants and moving them to the Home conference (interactively or using the right-click menu).
- The operator can move one or several participants from an ongoing conference to the *Operator conference* for a private conversation.

- The operator can move participants between ongoing Continuous Presence conferences.

Operator Conference Guidelines

- An *Operator conference* can only run in Continuous Presence mode.
- *Operator conference* is defined in the Conference Profile. When enabled in Conference Profile, *High Definition Video Switching* option is disabled.
- An *Operator conference* can only be created by a User with Operator or Administrator *Authorization* level.
- *Operator conference* name is derived from the User Login Name and it cannot be modified.
- Only one *Operator conference* per User *Login Name* can be created.
- When created, the *Operator conference* must include one and only one participant - the Operator participant.
- Only a defined dial-out participant can be added to an *Operator conference* as an Operator participant
- Once running, the Collaboration Server user can add new participants or move participants from other conferences to this conference. The maximum number of participants in an *Operator conference* is the same as in standard conferences.
- Special icons are used to indicate an *Operator conference* in the Ongoing Conferences list and the operator participant in the Participants list.
- An *Operator conference* cannot be defined as a Reservation.
- An *Operator conference* can be saved to a Conference Template. An ongoing *Operator conference* can be started from a Conference Template.
- The Operator participant cannot be deleted from the *Operator conference* or from any other conference to which she/he was moved to, but it can be disconnected from the conference.
- When deleting or terminating the *Operator conference*, the operator participant is automatically disconnected from the MCU, even if participating in a conference other than the *Operator conference*.
- Moving participants from/to an *Operator conference* follows the same guidelines as moving participants between conferences. For move guidelines, see "*Move Guidelines*" on page **10-15**.
- When a participant is moved from the Entry Queue to the *Operator conference*, the option to move back to the source (Home) conference is disabled as the Entry Queue is not considered as a source conference.
- The conference chairperson cannot be moved to the *Operator conference* following the individual help request if the *Auto Terminate When Chairperson Exits* option is enabled, to prevent the conference from automatically ending prematurely. In such a case, the assistance request is treated by the system as a conference assistance request, and the operator can join the conference.

Defining the Components Enabling Operator Assistance

To enable operator assistance for conferences, the following conferencing entities must be adjusted or created:

- IVR Service (Entry Queue and Conference) in which Operator Assistance options are enabled.

- A Conference Profile with the *Operator Conference* option enabled.
- An active Operator conference with a connected Operator participant.

Defining a Conference IVR Service with Operator Assistance Options

In the *RMX Management* pane, expand the *Rarely Used* list and click the **IVR Services** (▦) entry.

1 On the *IVR Services* toolbar, click the **New Conference IVR Service** (▦) button.

The *New Conference IVR Service - Global* dialog box opens.
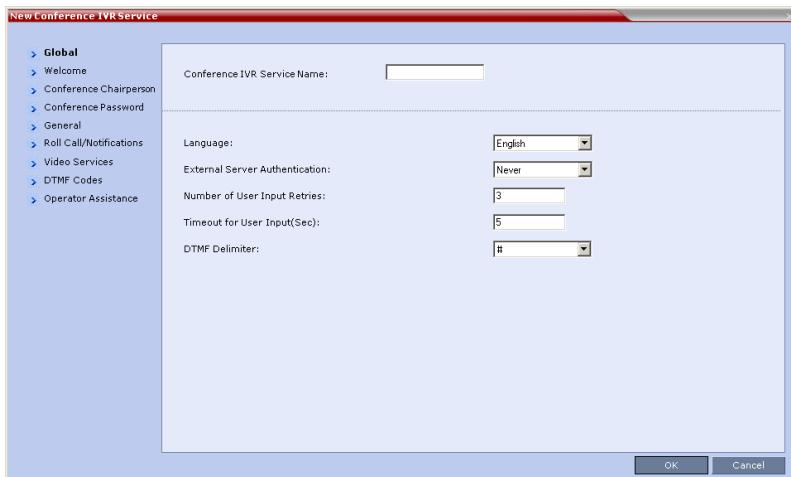
2 Enter the *Conference IVR Service Name*.

3 Define the *Conference IVR Service - Global* parameters. For more information, see *Table 15-3, "Conference IVR Service Properties - Global Parameters,"* on page **15-7**.

4 Click the **Welcome** tab.
The *New Conference IVR Service - Welcome* dialog box opens.

5 Define the system behavior when the participant enters the Conference IVR queue. For more information, see "*Defining a New Conference IVR Service*" on page **15-6**.

6 Click the **Conference Chairperson** tab.
The *New Conference IVR Service - Conference Chairperson* dialog box opens.

7 If required, enable the chairperson functionality and select the various voice messages and options for the chairperson connection. For more information, see *Table 15-4, "New Conference IVR Service Properties - Conference Chairperson Options and Messages,"* on page **15-9**.

8 Click the **Conference Password** tab.

The *New Conference IVR Service - Conference Password* dialog box opens.

9 If required, enable the request for conference password before moving the participant from the conference IVR queue to the conference and set the MCU behavior for password request for *Dial-in* and *Dial-out* participant connections. For more information, see *Table 15-5, "New Conference IVR Service Properties - Conference Password Parameters,"* on page **15-10**.

10 Select the various audio messages that will be played in each case. For more information, see *Table 15-5, "New Conference IVR Service Properties - Conference Password Parameters,"* on page **15-10**.

11 Click the **General** tab.

The *New Conference IVR Service - General* dialog box opens.

12 Select the messages that will be played during the conference. For more information, see *Table 15-6, "Conference IVR Service Properties - General Voice Messages,"* on page **15-11**.

13 Click the **Video Services** tab.

The *New Conference IVR Service - Video Services* dialog box opens.

14 Define the *Video Services* parameters. For more information, see *Table 15-8, "New Conference IVR Service Properties - Video Services Parameters,"* on page **15-15**.

15 Click the **DTMF Codes** tab.
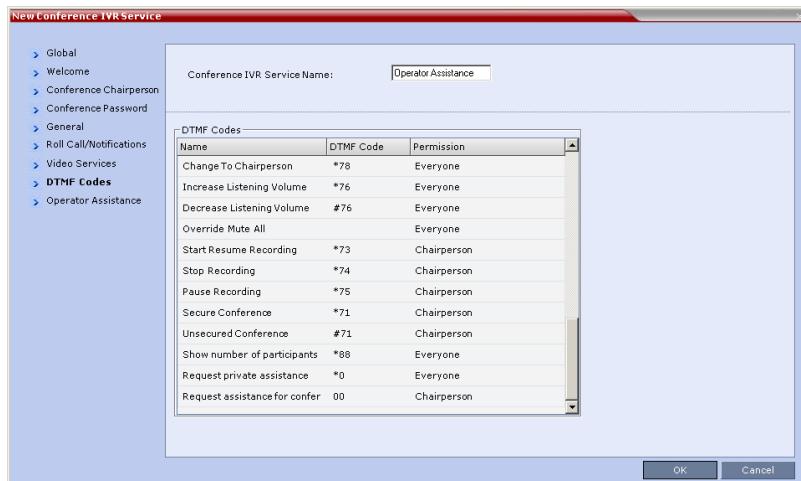
The *New Conference IVR Service - DTMF Codes* dialog box opens.

The default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson are listed. For the full list of the available DTMF codes, see *Table 15-9, "New Conference IVR Service Properties - DTMF Codes,"* on page **15-16**.

16 If required, modify the default DTMF codes and the permissions for various operations including Operator Assistance options:

— ***0** for individual help - the participant requested help for himself or herself. In such a case, the participant requesting help is moved to the Operator conference for one-on-one conversation. By default, all participants can use this code.

— **00** for conference help - the conference chairperson (default) can request help for the conference. In such a case, the operator joins the conference.

17 Click the **Operator Assistance** tab.

The *Operator Assistance* dialog box opens.
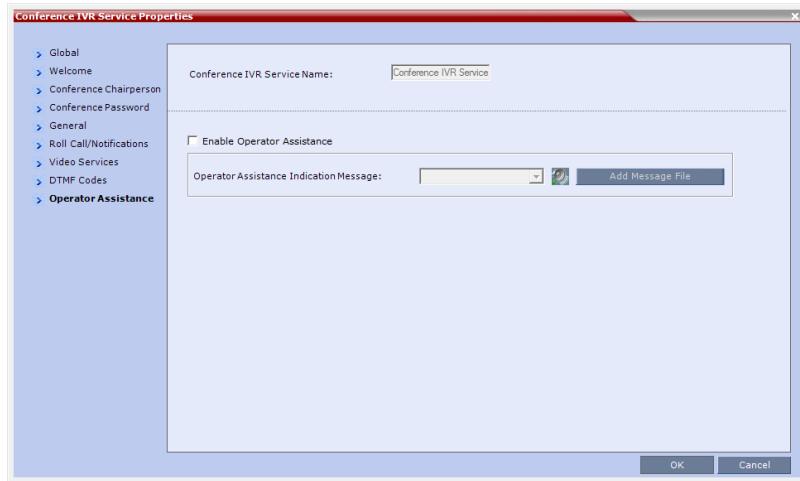
18 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process to the conference or during the conference.

19 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for the operator's assistance.

> If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

20 Click **OK** to complete the IVR Service definition.
The new Conference IVR Service is added to the *IVR Services* list.

Defining an Entry Queue IVR Service with Operator Assistance Options

1 In the *RMX Management* pane, click **IVR Services** (📇).

2 In the *IVR Services* list, click the **New Entry Queue IVR Service** (📇) button.

The *New Entry Queue IVR Service - Global* dialog box opens.

3 Define the *Entry Queue Service Name*.

4 Define the Entry Queue IVR Service Global parameters. For more information, see Table 15-10, "*Entry Queue IVR Service Properties - Global Parameters,*" on page **15-19**.

5 Click the **Welcome** tab.
The *New Entry Queue IVR Service - Welcome* dialog box opens.

6 Define the system behavior when the participant enters the Entry Queue. *T*his dialog box contains options that are identical to those in the *Conference IVR Service - Welcome Message* dialog box.

7 Click the **Conference ID** tab.
The *New Entry Queue IVR Service - Conference ID* dialog box opens.

8 Select the required voice messages. For more information, see *Table 15-11, "Entry Queue IVR Service Properties - Conference ID,"* on page **15-21**.

9   Click the **Video Services** tab.
    The *New Entry Queue IVR Service - Video Services* dialog box opens.

10 In the *Video Welcome Slide* list, select the video slide that will be displayed to participants connecting to the Entry Queue. The slide list includes the video slides that were previously uploaded to the MCU memory.

11 Click the **Operator Assistance** tab.

    The *Operator Assistance* dialog box opens.

12 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.

13 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for operator's assistance.

> If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

14 Click **OK** to complete the Entry Queue IVR Service definition.
    The new Entry Queue IVR Service is added to the *IVR Services* list.

Defining a Conference Profile for an Operator Conference

1   In the *RMX Management* pane, click **Conference Profiles**.

2 In the *Conference Profiles* pane, click the **New Profile** button.
The *New Profile – General* dialog box opens.
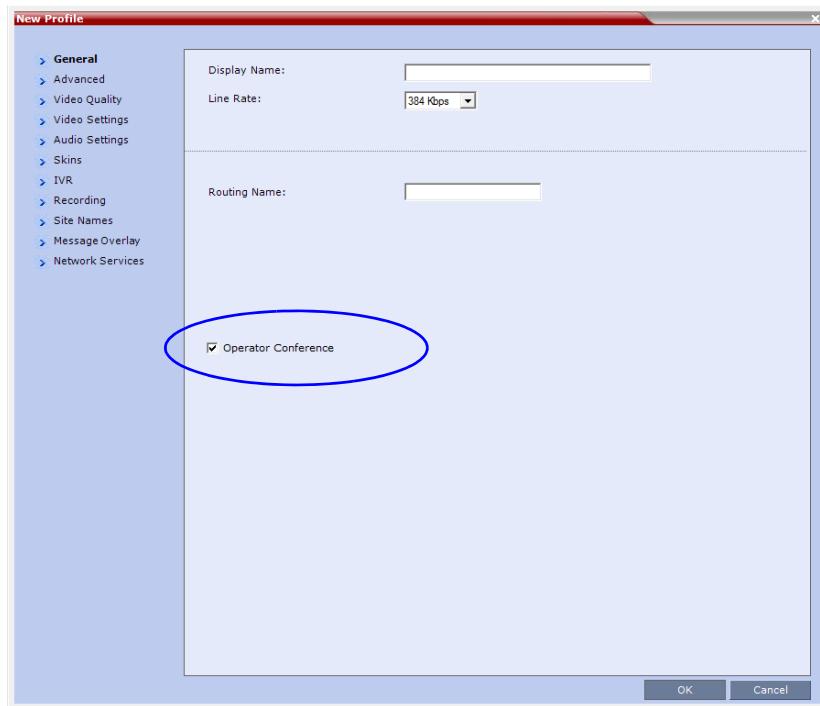
3 Define the Profile name and, if required, the Profile general parameters.
For more details, see "*New AVC-CP Profile - General Parameters*" on page **2-10**.

4 Click the **Operator Conference** check box.

5 Click the **Advanced** tab.

The *New Profile – Advanced* dialog box opens.
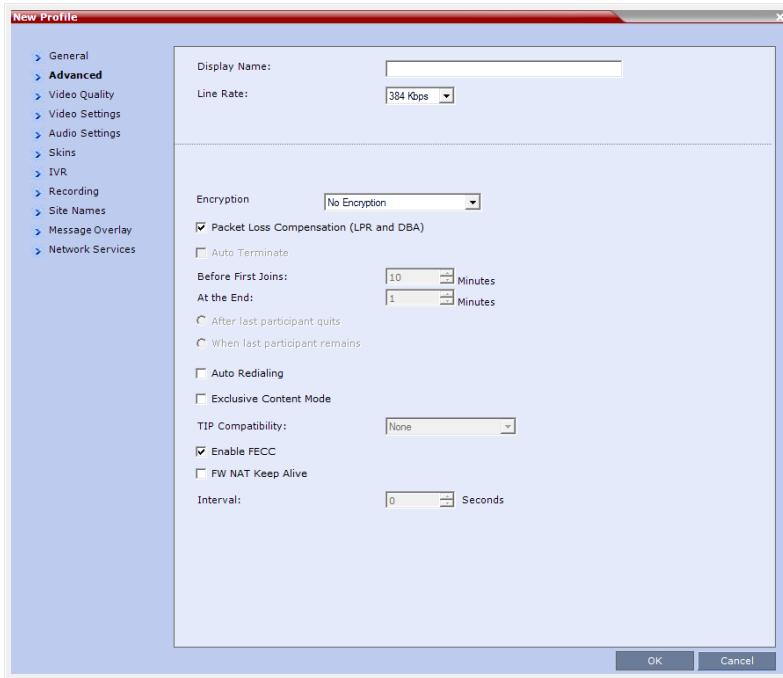
6   Define the Profile *Advanced* parameters. For more details, see Table 2-5, *"New AVC-CP Profile - Advanced Parameters"*.

Note that when Operator Conference is selected, the **Auto Terminate** selection is automatically cleared and disabled and the Operator conference cannot automatically end unless it is terminated by the Collaboration Server User.

7   Click the **Video Quality** tab.

The *New Profile – Video Quality* dialog box opens.

8   Define the Video Quality parameters. For more details, see Table 2-6, *"New AVC Profile - Video Quality Parameters"*.

9   Click the **Video Settings** tab.

The *New Profile - Video Settings* dialog box opens.

10 Define the video display mode and layout. For more details, see Table 2-7, *"New AVC CP Profile - Video Settings Parameters"*.

11 Define the remaining Profile parameters. For more details, see *Defining AVC - CP Conferencing Profiles*.

12 Click **OK** to complete the *Profile* definition.
A new *Profile* is created and added to the *Conference Profiles* list.

Starting an Ongoing Operator Conference

To start a conference from the Conference pane:

1   In the *Conferences* pane, click the **New Conference** (🔹) button.

The *New Conference – General* dialog box opens.

2 In the *Profile* field, select a Profile in which the *Operator Conference* option is selected.
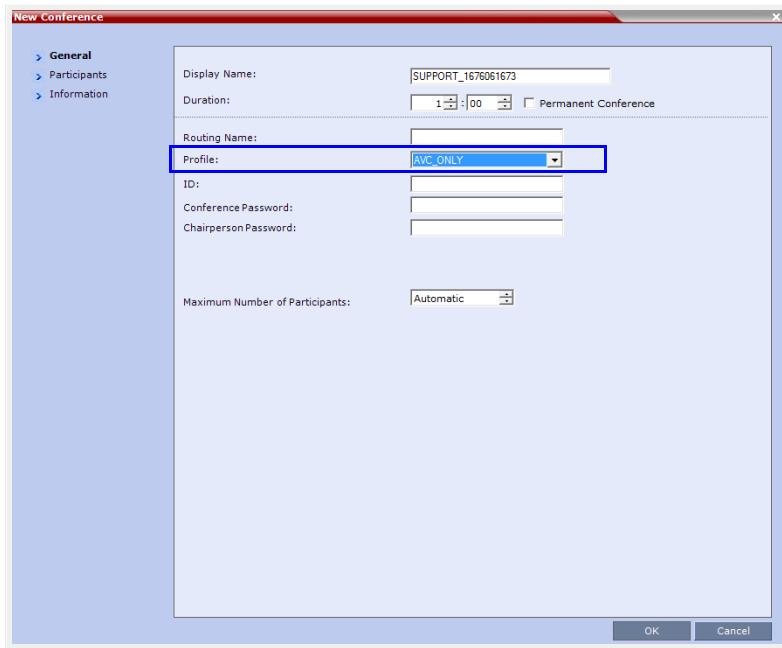
Upon selection of the *Operator Conference* Profile, the *Display Name* is automatically taken from the Collaboration Server User *Login Name*. This name cannot be modified.

Only one Operator conference can be created for each User Login name.

3 Define the following parameters:

Table 10-1 New Conference – General Options

Field	Description
Duration	Define the duration of the conference in hours using the format HH:MM (default 01:00). **Notes:** • The Operator conference is automatically extended up to a maximum of 168 hours. Therefore, the default duration can be used. • This field is displayed in all tabs.

Table 10-1 *New Conference – General Options (Continued)*

Field	Description
Routing Name	*Routing Name* is the name with which ongoing conferences, Meeting Rooms, Entry Queues and SIP Factories register with various devices on the network such as gatekeepers and SIP servers. This name must be defined using ASCII characters. **Comma, colon and semicolon characters cannot be used in the *Routing Name.*** The *Routing Name* can be defined by the user or automatically generated by the system if no *Routing Name* is entered as follows: • If ASCII characters are entered as the *Display Name*, it is used also as the *Routing Name* • If a combination of Unicode and ASCII characters (or full Unicode text) is entered as the *Display Name*, the *ID* (such as Conference ID) is used as the *Routing Name.* If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message and requests that you to enter a different name.
ID	Enter the unique-per-MCU conference ID. If left blank, the MCU automatically assigns a number once the conference is launched. This ID must be communicated to conference participants to enable them to dial in to the conference.
Conference Password	Leave this field empty when defining an Operator conference.
Chairperson Password	Leave this field empty when defining an Operator conference.
Maximum Number of Participants	Enter the maximum number of participants that can connect to an Operator conference (you can have more than two), or leave the default selection (Automatic). Maximum number of participants that can connect to an Operator conference:

4   Click the **Participants** tab.
The *New Conference - Participants* dialog box opens.

You must define or add the Operator participant to the Operator conference.

This participant must be defined as a **dial-out** participant.

Define the parameters of the endpoint that will be used by the Collaboration Server User to connect to the Operator conference and to other conference to assist participants.

For more details, see the *Polycom RMX 1800 Getting Started Guide*, *"Participants Tab"* on page **3-16**.

5   **Optional**. Click the **Information** tab**.**
The *Information* tab opens.

6   Enter the required information. For more details, see the *Polycom RMX 1800 Getting Started Guide*, *"Information Tab"* on page **3-18**.

7   Click **OK**.

The new Operator conference is added to the ongoing *Conferences* list with a special icon .

The Operator participant is displayed in the *Participants* list with an Operator participant icon , and the system automatically dials out to the Operator participant.

Saving an Operator Conference to a Template

The Operator conference that is ongoing can be saved as a template.

To save an ongoing Operator conference as a template:

1 In the *Conferences List*, select the Operator conference you want to save as a Template.

2 Click the **Save Conference to Template** ( ) button.
or
Right-click and select **Save Conference to Template**.

The conference is saved to a template whose name is taken from the ongoing conference *Display Name* (the Login name of the Collaboration Server User). The Template is displayed with the Operator Conference icon.

Starting an Operator Conference from a Template

An ongoing Operator conference can be started from an Operator Template saved in the *Conference Templates* list.

To start an ongoing Operator conference from an Operator Template:

1   In the *Conference Templates* list, select the Operator Template to start as an ongoing Operator conference.

- • You can only start an Operator conference from a template whose name is identical to your Login Name. For example, if your Login name is Polycom, you can only start an Operator conference from a template whose name is Polycom.
- • If an ongoing Operator conference with the same name or any other conference with the same ID is already running, you cannot start another Operator conference with the same login name.

2   Click the **Start Conference from Template** (🗐) button.
    or
    Right-click and select **Start Conference from Template**.

The conference is started.

The name of the ongoing conference in the *Conferences* list is taken from the Conference Template *Display Name*.

Monitoring Operator Conferences and Participants Requiring Assistance

Operator conferences are monitored in the same way as standard ongoing conferences. Each Operator conference includes at least one participant - the Operator.

You can view the properties of the *Operator conference* by double-clicking the conference entry in the *Conferences* list or by right-clicking the conference entry and selecting **Conference Properties**. For more information, see the *Polycom RMX 1800 Getting Started Guide*, *"Conference Level Monitoring"* on page **3-32**.

Requesting Help

A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device. The participant can request *Individual Assistance* (default DTMF code ***0**) or *Conference Assistance* (default DTMF code **00**).

Participants in Entry Queues who failed to enter the correct destination conference ID or the conference password will wait for operator assistance (provided that an Operator conference is active).

When requiring or requesting operator assistance, the Collaboration Server management application displays the following:

- The participant's connection *Status* changes, reflecting the help request. For more information, see Table 10-2.
- The conference status changes and it is displayed with the exclamation point icon and the status "Awaiting Operator".
- The appropriate voice message is played to the relevant participants indicating that assistance will be provided shortly.

The following icons and statuses are displayed in the *Participant Status* column:

Table 10-2 Participants List Status Column Icons and Indications

Icon	Status Indication	Description
	Awaiting Individual Assistance	The participant has requested the operator's assistance for himself/herself.
	Awaiting Conference Assistance	The participant has requested the operator's assistance for the conference. Usually this means that the operator is requested to join the conference.

When the Operator moves the participant to the *Operator conference* for individual assistance the participant Status indications are cleared.

Participant Alerts List

The *Participant Alerts* list contains all the participants who are currently waiting for operator assistance.

Participants are automatically added to the *Participants Alerts* list in the following circumstances:

• The participant fails to connect to the conference by entering the wrong conference ID or conference password and waits for the operator's assistance

• The participant requests Operator's Assistance during the ongoing conference

This list is used as reference only. Participants can be assisted and moved to the *Operator conference* or the destination conference only from the *Participants* list of the Entry Queues or ongoing conference where they are awaiting assistance.

The participants are automatically removed from the *Participant Alerts* list when moved to any conference (including the *Operator conference*).

Audible Alarms

In addition to the visual cues used to detect events occurring on the Collaboration Server, an audible alarm can be activated and played when participants request Operator Assistance.

Using Audible Alarms

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU in either the Collaboration Server Web Client or RMX Manager.

The Audible Alarm played when Operator Assistance is requested is enabled and selected in the **Setup > Audible Alarm > User Customization**. When the Audible Alarm is activated, the *.wav file selected in the *User Customization* is played, and it is repeated according to the number of repetitions defined in the *User Customization*.

If more than one Collaboration Server is monitored in the *RMX Manager*, the Audible Alarm must be enabled separately for each Collaboration Server installed in the site/configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, the Audible Alarms are synchronized and played one after the other. It is important to note that when *Stop Repeating Alarm* is selected from the toolbar from the Collaboration Server Web Client or RMX Manager, all activated Audible Alarms are immediately halted.

For more details on Audible alarms and their configuration, see "*Audible Alarms"* on page **19-29**.

Moving Participants Between Conferences

The Collaboration Server User can move participants between ongoing conferences, including the *Operator conference*, and from the Entry Queue to the destination conference if help is required.

When moving between conferences or when a participant is moved from an Entry Queue to a conference by the Collaboration Server user (after failure to enter the correct destination ID or conference password), the IVR messages and slide display are skipped.

Move Guidelines

* Move between conferences can be performed without an active *Operator conference*.
* When moving the conference chairperson from his/her conference to another conference, the source conference will automatically end if the *Auto Terminate When Chairperson Exits* option is enabled and that participant is the only conference chairperson.
* When moving the Operator to any conference (following assistance request), the IVR messages and slide display are skipped.
* Participants cannot be moved from LPR-enabled conferences to non-LPR conferences. Move from non-LPR conferences to LPR-enabled conferences is available.
* Move between encrypted and non-encrypted conferences depends on the **ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF** flag setting, as described in Table 10-3:

Table 10-3 *Participant Move Capabilities vs. ALLOW_NON_ ENCRYPT_PARTY_IN_ENCRYPT_CONF flag setting*

Flag Setting	Source Conference/ EQ Encrypted	Destination Conference Encrypted	Move Enabled?
NO	Yes	Yes	Yes
NO	Yes	No	Yes
NO	No	Yes	No
NO	No	No	Yes
YES	Yes	Yes	Yes
YES	Yes	No	Yes

Table 10-3 *Participant Move Capabilities vs. ALLOW_NON_*
ENCRYPT_PARTY_IN_ENCRYPT_CONF flag setting (Continued)

Flag Setting	Source Conference/ EQ Encrypted	Destination Conference Encrypted	Move Enabled?
YES	No	Yes	Yes
YES	No	No	Yes

- When moving dial-out participants who are disconnected to another conference, the system automatically dials out to connect them to the destination conference.
- Cascaded links cannot be moved between conferences.
- Participants cannot be moved to a conference if the move will cause the number of participants to exceed the maximum number of participants allowed for the destination conference.

Moving Participants Options

Collaboration Server users can assist participants by performing the following operations:

- Move a participant to an *Operator conference* (Attend a participant).
- Move a participant to the Home (destination) conference.
- Move participant from one ongoing conference to another

A move can be performed using the following methods:

- Using the participant right-click menu
- Using drag and drop

To move a participant from the ongoing conference using the right-click menu options:

1 In the *Conferences* list, click the conference where there are participants waiting for Operator's Assistance to display the list of participants.

2 In the *Participants* list, right-click the icon of the participant to move and select one of the following options:

Disconnect Participant
Delete Participant
Mute Audio
Suspend Video
Block Audio
Change to Chairperson
Change To Content Token Owner
Add Participant to Address Book
Start Recording ▶
Quick Search
View Participant Sent Video
View Participant Received Video
Request Intra for Received Video
Request Intra for Sent Video
Request Intra for Received+Sent Video
Copy Participant
Cut Participant
Participant Debug Info
Send Text Message To Participant
Participant Properties

— **Move to Operator Conference** - to move the participant to the Operator conference.
— **Move to Conference** - to move the participant to any ongoing conference.

When selected, the *Move to Conference* dialog box opens, letting you select the name of the destination conference.

— **Back to Home Conference** - if the participant was moved to another conference or to the *Operator conference*, this options moves the participant back to his/her source conference.

This option is not available if the participant was moved from the Entry Queue to the *Operator conference* or the destination conference.

Moving a Participant Interactively

You can drag and drop a participant from the Entry Queue or ongoing conference to the Operator or destination (Home) conference:

1 Display the participants list of the Entry Queue or the source conference by clicking its entry in the *Conferences* list.

2 In the Participants list, drag the icon of the participant to the *Conferences List* pane and drop it on the *Operator Conference* icon or another ongoing conference.

11

Conference Templates

Conference Templates enable administrators and operators to create, save, schedule and activate identical conferences.

A *Conference Template*:

- Saves the conference Profile.
- Saves all participant parameters including their *Personal Layout* and *Video Forcing* settings.

Guidelines

- The maximum number of templates is 100.

  Trying to start a *Conference Template* that exceeds the allowed maximum number of participants will result in participants being disconnected due to resource deficiency.

- If the Profile assigned to a conference is deleted while the conference is ongoing the conference cannot be saved as a template.

- A Profile assigned to a *Conference Template* cannot be deleted. The system does not permit such a deletion.

- Profile parameters are not embedded in the *Conference Template*, and are taken from the Profile when the *Conference Template* becomes an ongoing conference. Therefore, any changes to the Profile parameters between the time the *Conference Template* was created and the time that it is activated (and becomes an ongoing conference) will be applied to the conference.

- Only defined participants can be saved to the *Conference Template*. Before saving a conference to a template ensure that all undefined participants have disconnected.

- Undefined participants are not saved in *Conference Templates*.

- Participant properties are embedded in the *Conference Template* and therefore, if the participant properties are modified in the Address Book after the *Conference Template* has been created they are not applied to the participant whether the *Template* becomes an ongoing conference or not.

- The *Conference Template* display name, routing name or ID can be the same as an Ongoing Conference, reservation, Meeting Room or Entry Queue as it is not active. However, an ongoing conference cannot be launched from the *Conference Template* if an ongoing conference, Meeting Room or Entry Queue already has the same name or ID. Therefore, it is recommended to modify the template ID, display name, routing name to be unique.

- A *Reservation* that has become an ongoing conference can be saved as *Conference Template*.

- SIP Factories and Entry Queues cannot be saved as *Conference Templates*.

- The conference specified in the *Conference Template* can be designated as a *Permanent Conference*. For more information see "*Lecture Mode*" on page **4-38**.

Using Conference Templates

The *Conference Templates* list is initially displayed as a closed tab in the *Collaboration Server Web Client* main window. The number of saved *Conference Templates* is indicated on the tab.

Conference Templates Tab

Number of Saved Conference Templates
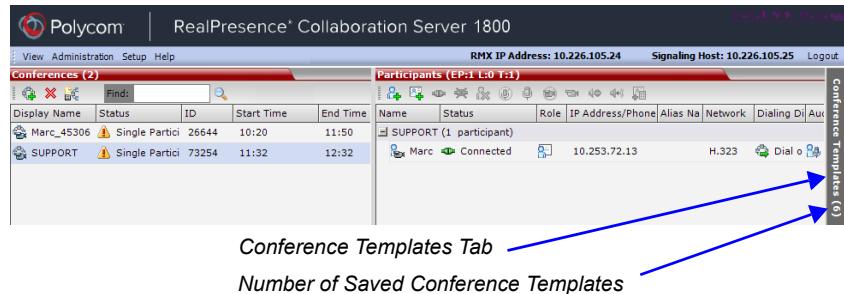
Clicking the tab opens the *Conference Templates* list.

Toolbar buttons

Click to hide the Conference Templates List

List of Saved Templates

Number of Saved Conference Templates
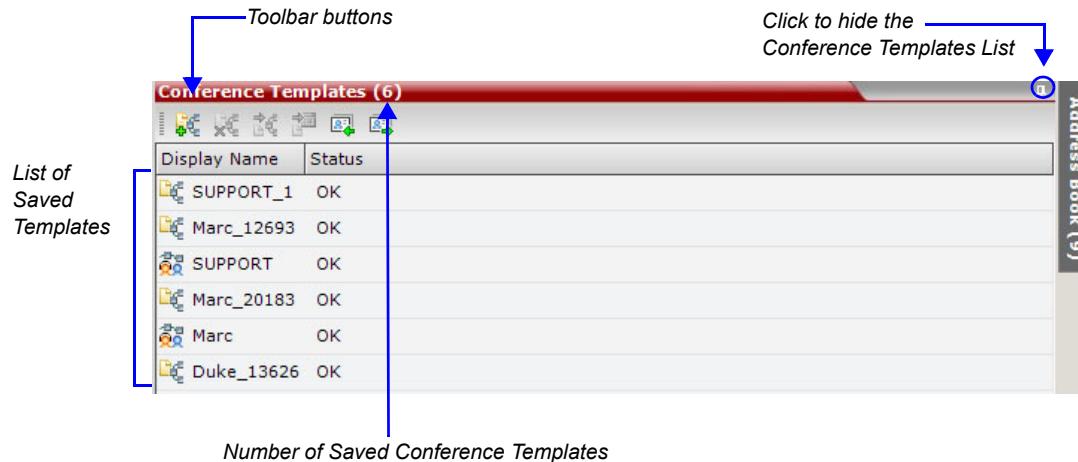
The *Conference Templates* are listed by *Conference Template Display Name* and *ID* and can be sorted by either field. The list can be customized by re-sizing the pane, adjusting the column widths or changing the order of the column headings.

For more information see *Polycom RMX 1800 Getting Started Guide, "Customizing the Main Screen"* on page **3-10**.

Clicking the anchor pin (⊙) button hides the *Conference Templates* list as a closed tab.

Toolbar Buttons

The *Conference Template* toolbar includes the following buttons:

Table 1 Conference Templates – Toolbar Buttons

Button	Description
New Conference Template	Creates a new Conference Template.
Delete Conference Template	Deletes the Conference Template(s) that are selected in the list.

Table 1 *Conference Templates – Toolbar Buttons (Continued)*

Button	Description
Start Conference from Template	Starts an ongoing conference from the *Conference Template* that has an identical name, ID parameters and participants as the template.
Schedule Reservation from Template	Creates a conference Reservation from the Conference Template with the same name, ID, parameters and participants as the Template. Opens the *Scheduler* dialog box enabling you to modify the fields required to create a single or recurring *Reservation* based on the template. For more information see "*Reservations"* on page **9-1**.

The ***Conferences List*** toolbar includes the following button:

Table 2 *Conferences List – Toolbar Button*

Button	Description
Save Conference to Template	Saves the selected ongoing conference as a Conference Template.

Creating a New Conference Template

There are two methods to create a *Conference Template*:

- From scratch - defining the conference parameters and participants
- Saving an ongoing conference as Template

Creating a new Conference Template from Scratch

To create a new Conference Template:

1 In the *Collaboration Server Web Client*, click the **Conference Templates** tab.

2 Click the **New Conference Template** ( ) button.

The *New Conference Template - General* dialog box opens.

3 The fields of the *New Template – General* dialog box are identical to those of the *New Conference – General* dialog box. For a full description of the fields see the *Polycom RMX 1800 Getting Started Guide, "General Tab"* on page **3-14**.

4 Modify the fields of the *General* tab.

> A unique dial-in number must be assigned to each conferencing entity. However, Conference Templates can be assigned dial-in numbers that are already assigned to other conferencing entities, but when the template is used to start an ongoing conference or schedule a reservation, it will not start if another ongoing conference, Meeting Room, or Entry Queue is using this number.

5 Click the **Participants** tab.

The *New Template – Participants* dialog box opens.
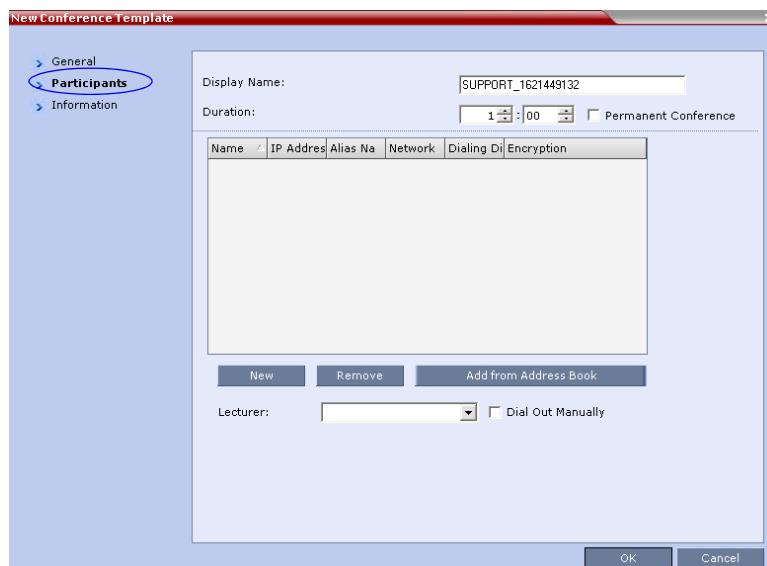
The fields of the *New Template – Participants* dialog box are the same as those of the *New Conference – Participant* dialog box.

For a full description of these fields see the *Polycom RMX 1800 Getting Started Guide, "Participants Tab"* on page **3-16**.

6 **Optional.** Add participants to the template from the *Address Book*.

7 Click the **New** button.

The *New Participant – General* tab opens.

The *New Template – Participant* dialog box remains open in the background.
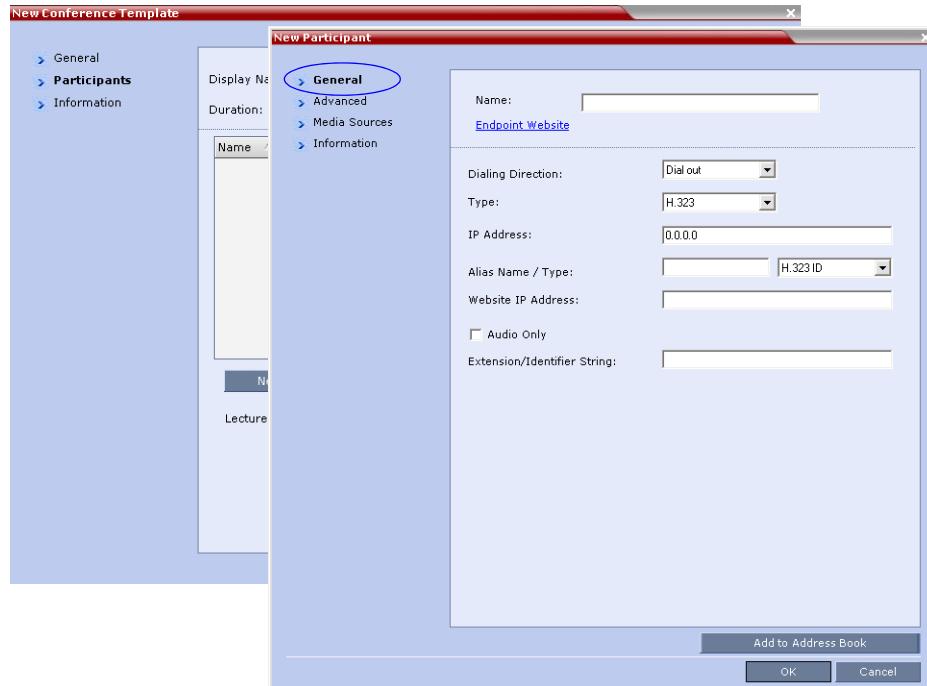
For a full description of the *General* tab fields see "*Adding a New participant to the Address Book Directly"* on page **8-8**.

8 Modify the fields of the *General* tab.

9 Click the **Advanced** tab.

The *New Participant – Advanced* tab opens.

For a full description of the *Advanced* tab fields see, "*New Participant – Advanced Properties"* on page **8-12**.

10 Modify the fields of the *Advanced* tab.

11 Click the **Media Sources** tab.

The *Media Sources* tab opens.

The *Media Sources* tab enables you to set up and save *Personal Layout* and *Video Forcing* settings for each participant.

For a full description of *Personal Layout* and *Video Forcing* settings see the *Polycom RMX 1800 Getting Started Guide, "Changing the Video Layout of a Conference"* on page **3-46** and "*Video Forcing (AVC-Based CP Conferences)"* on page **3-47**.

12 Modify the *Personal Layout* and *Video Forcing* settings for the participant.

13 **Optional.** Click the **Information** tab.

The *New Participant – Information* tab opens.
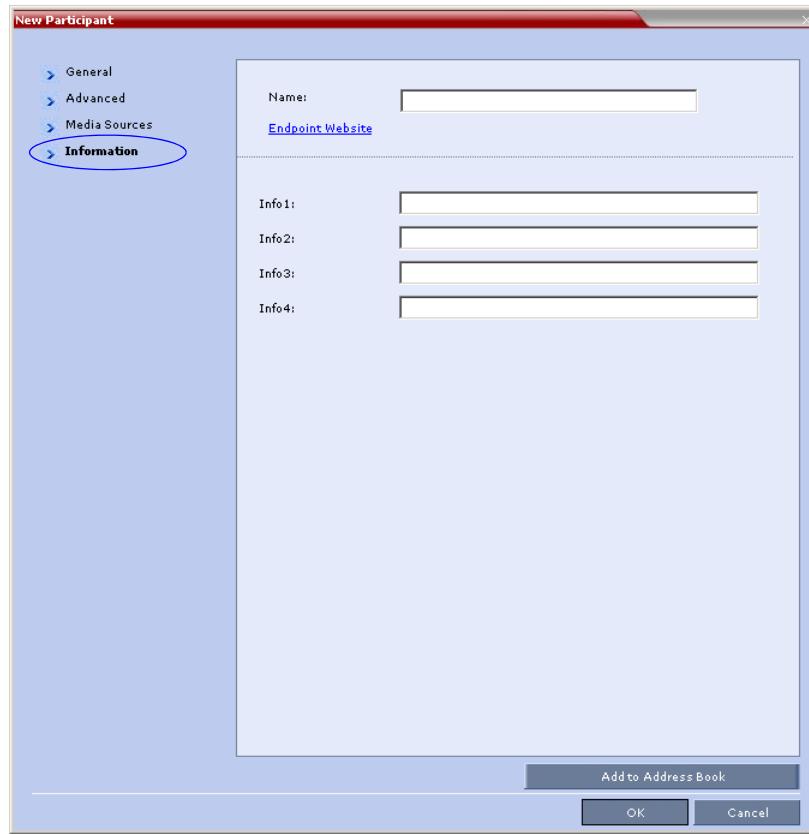
For a full description of the *Information* fields see the *Polycom RMX 1800 Getting Started Guide, "Information Tab"* on page **3-18**.

14 Click the **OK** button.

The participant you have defined is added to the *Participants List*.

The New Participant dialog box closes and you are returned to the *New Template – Participant* dialog box (which has remained open since Step 7).

15 **Optional.** In the *New Conference Template* dialog box, click the **Information** tab.

The *New Conference Template – Information* tab opens.
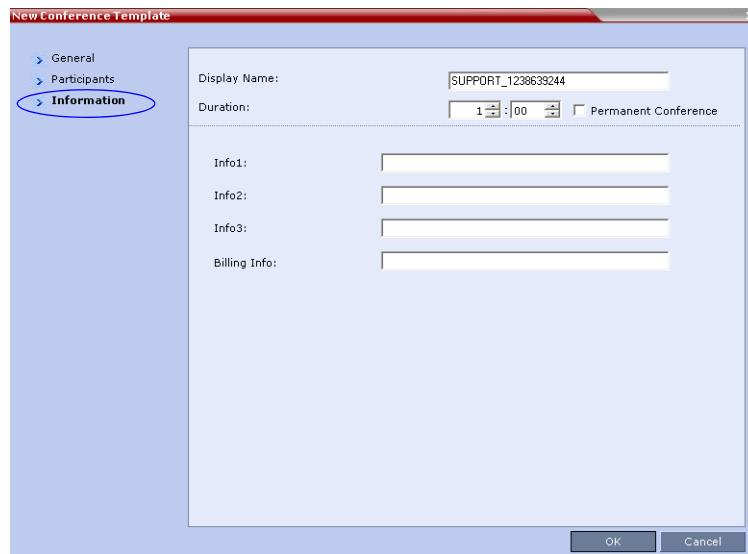
For a full description of the *Information* fields see the *Polycom RMX 1800 Getting Started Guide,* "*Information Tab*" on page **18**.

16 Click the **OK** button.

The *New Conference Template* is created and its name is added to the *Conference Templates* list.

Saving an Ongoing or AVC-based CP Operator Conference as a Template

Any ongoing or AVC-based CP *Operator Conference* can be saved as a template.

To save an ongoing or AVC-based CP Operator Conference as a template:

1 In the *Conferences List*, select the conference or *Operator Conference* to be saved as a Template.

2 Click the **Save Conference to Template** ( ) button.
or
Right-click and select **Save Conference to Template**.
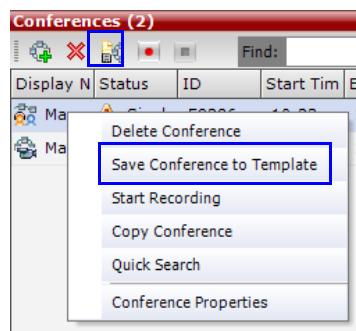
The conference is saved to a template whose name is taken from the ongoing conference *Display Name* (the *Login* name of the *Collaboration Server User*). The *Template* is displayed with the *Operator Conference* icon.
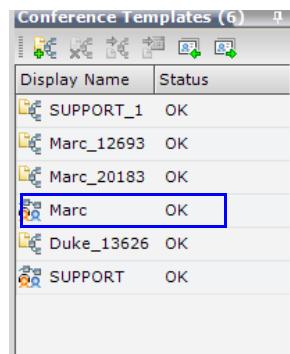
Starting an Ongoing Conference From a Template

An ongoing conference can be started from any Template saved in the *Conference Templates* list.

To start an ongoing conference from a Template:

1 In the *Conference Templates* list, select the Template you want to start as an ongoing conference.

2 Click the **Start Conference from Template** ( ) button.
or
Right-click and select **Start Conference from Template**.
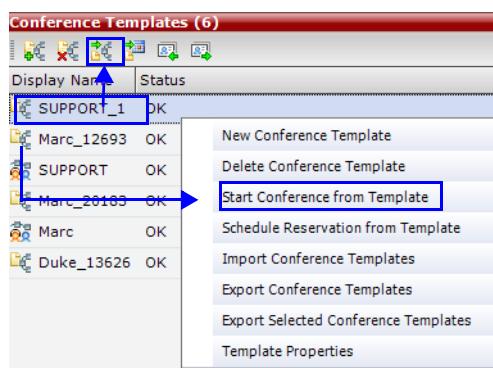
The conference is started.

The name of the ongoing conference in the *Conferences* list is taken from the Conference Template *Display Name*.

Participants that are connected to other ongoing conferences when the template becomes an ongoing conference are not connected.

If an ongoing conference, Meeting Room or Entry Queue with the same *Display Name, Routing Name* or *ID* already exists in the system, the conference will not be started.

Starting an Operator Conference from a Template (AVC Conferencing)

An ongoing Operator conference can be started from an Operator Template saved in the *Conference Templates* list.

To start an ongoing Operator conference from an Operator Template:

1 In the *Conference Templates* list, select the Operator Template to start as an ongoing Operator conference.

> • You can only start an Operator conference from a template whose name is identical to your Login Name. For example, if your Login name is Polycom, you can only start an Operator conference from a template whose name is Polycom.
>
> • If an ongoing Operator conference with the same name or any other conference with the same ID is already running, you cannot start another Operator conference with the same login name.

2 Click the **Start Conference from Template** (⊞) button.

or

Right-click and select **Start Conference from Template**.

The conference is started.

The name of the ongoing conference in the *Conferences* list is taken from the Conference Template *Display Name*.

Scheduling a Reservation From a Conference Template

A *Conference Template* can be used to schedule a single or recurring *Reservation*.

To schedule a Reservation from a Conference Template:

1 In the *Conference Templates* list, select the Conference Template you want to schedule as a Reservation.

2 Click the **Schedule Reservation from Template** ( ) button.

or

Right-click and select **Schedule Reservation from Template**.
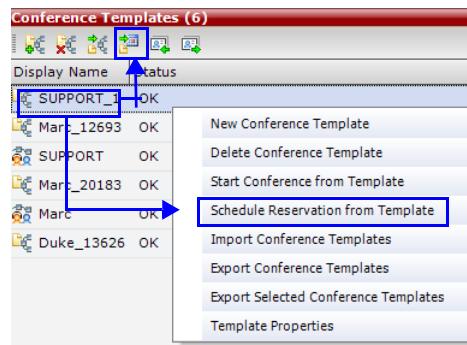
The *Reservation Properties* dialog box is displayed.

The *Display Name* of the *Reservation* is taken from the Conference Template *Display Name*.

Conference Template and Reservation Name
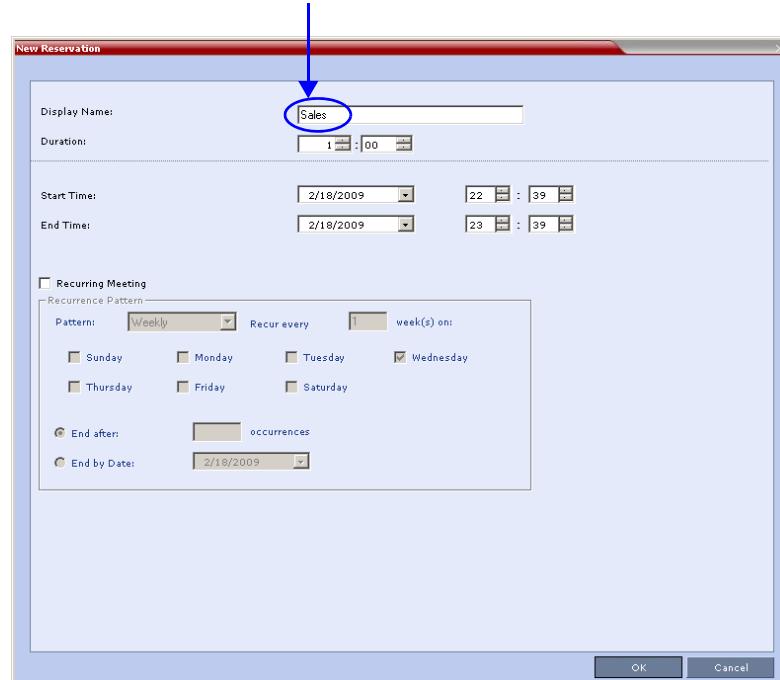
For a full description of the *Reservation Properties* fields see Table 9-2, "*New Reservation – Schedule Tab,*" on page **9-11**.

3 Modify the fields of the *Reservation Properties*.

4 Click the **OK** button.

A *Reservation* is created based on the *Conference Template*. The *Reservation* can be viewed and modified along with all other *Reservations* using the *Reservations - Calendar View* and *Reservations List*.

If you create a recurring reservation all occurrences have the same ID.

The series number (_0000n) of each reservation is appended to its *Display Name*.

Example:

Conference Template name: Sales

Display Name for single scheduled occurrence: Sales

If 3 recurrences of the reservation are created:

Display Name for occurrence 1:   Sales_**00001**

Display Name for occurrence 2:   Sales_**00002**

Display Name for occurrence 3:   Sales_**00003**

Deleting a Conference Template

One or several *Conference Templates* can be deleted at a time.

To delete Conference Templates:

1 In the *Conference Templates* list, select the *Template(s)* you want to delete.

2 Click the **Delete Conference Template** (🖳) button.
or
Right-click and select **Delete Conference Template**.
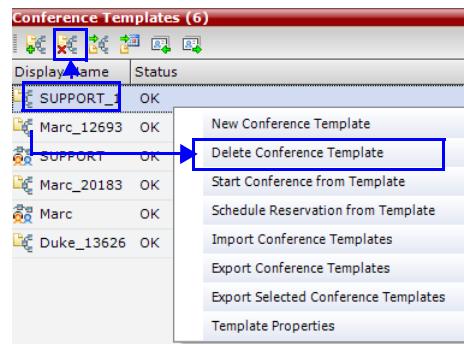
A confirmation dialog box is displayed.

3 Click the **OK** button to delete the *Conference Template(s)*.

Exporting and Importing Conference Templates

Conference Templates can be exported from one MCU and imported to multiple MCUs in your environment. Additionally, you can export *Conference Templates* and their associated *Conference Profiles* simultaneously. Using this option can save configuration time and ensures that identical settings are used for conferences running on different MCUs. This is especially important in environments using cascading conferences that are running on different MCUs.

• Administrators can export and import *Conference Templates*. Operators are only allowed to export *Conference Templates*.

• You can select a single, multiple or all *Conference Templates* to be exported.

- Both *Conference Templates* and their associated *Conference Profiles* can be exported and imported simultaneously when enabling the **Export includes conference profiles** or **Import includes conference profiles** options.
- Exporting and importing *Conference Templates* only can be used when you want to export and import individual *Conference Templates* without their associated Conference Profiles. This option enables you to import *Conference Templates* when *Conference Profiles* already exist on an MCU.

Exporting Conference Templates

Conference Templates are exported to a single XML file that can be used to import the *Conference Templates* on multiple MCUs.

Using the *Export Conference Templates* option, you can:

- Export all *Conference Templates* from an MCU
- Export selected *Conference Templates*

Exporting All Conference Templates from an MCU

To export all Conference Templates from an MCU:

1 In the *Collaboration Server Web Client* main window, click the *Conference Templates* tab.

The *Conference Templates* list pane is displayed.
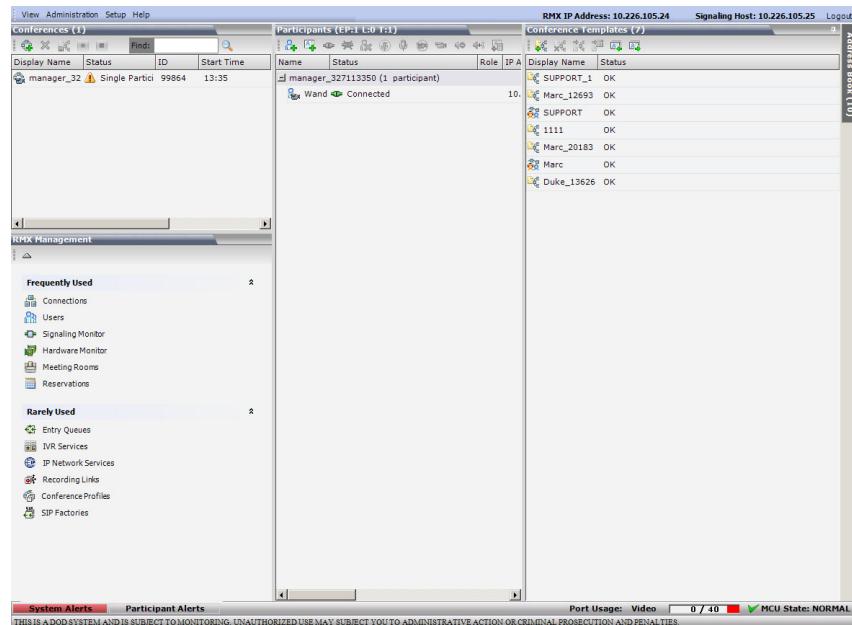
2 Click the **Export Conference Templates** button or right-click the *Conference Templates* list, and then click **Export Conference Templates**.

The *Conference Templates - Export* dialog box is displayed.

3 In the *Export Path* field, type the path name to the location where you want to save the exported file or click **Browse** to select the desired path.

4 Optional. Clear the **Export includes conference profiles** check box when you only want to export *Conference Templates*.

When this check box is cleared, the *Conference Templates - Export* dialog box is displayed without the *Profiles file name* field.

5 In the *Templates file name* field, type the file name prefix. The file name suffix (_confTemplates.xml) is predefined by the system. For example, if you type *Templates01*, the exported file name is defined as *Templates01_confTemplates.xml*.

The system automatically defines the *Profiles file name* field with the same file name prefix as the *Templates file name* field. For example, if you type *Templates01* in the *Templates file name* field, the exported profiles file name is defined as *Templates01_confProfiles.xml*.

6 Click **OK** to export the *Conference Templates* and *Conference Profiles* to a file.

Exporting Selected Conference Templates

You can export a single *Conference Template* or multiple *Conference Templates* to other MCUs in your environment.

To export selected Conference Templates:

1 In the *Conference Templates* list, select the templates you want to export.

2 Right-click the *Conference Templates* to be exported, and then click **Export Selected Conference Templates**.

The *Conference Templates - Export* dialog box is displayed.

3 In the *Export Path* field, type the path name to the location where you want to save the exported file or click **Browse** to select the desired path.

4 Optional. Clear the **Export includes conference profiles** check box when you only want to export Conference Templates.

When this check box is cleared, the *Conference Templates - Export* dialog box is displayed without the *Profiles file name* field.

5 In the *Templates file name* field, type the file name prefix. The file name suffix (_confTemplates.xml) is predefined by the system. For example, if you type, *Templates01*, the exported file name is defined as *Templates01_confTemplates.xml*.

The system automatically defines the *Profiles file name* field with the same file name prefix as the *Templates file name* field. For example, if you type *Templates01* in the *Templates file name* field, the exported profiles file name is defined as *Templates01_confProfiles.xml*.

6 Click **OK** to export the *Conference Templates* and *Conference Profiles* to a file.

Importing Conference Templates

You can import *Conference Templates* and *Conference Profiles* from one MCU to multiple MCUs in your environment.

To import Conference Templates:

1 In the *Collaboration Server Web Client* main window, click the *Conference Templates* tab.

The *Conference Templates* are displayed.

2 Click the **Import Conference Templates** button or right-click the Conference Templates pane, and then click I**mport Conference Templates.**
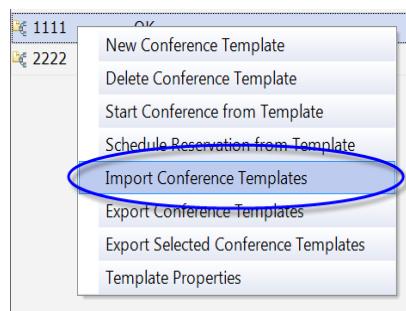
The *Conference Templates - Import* dialog box is displayed.
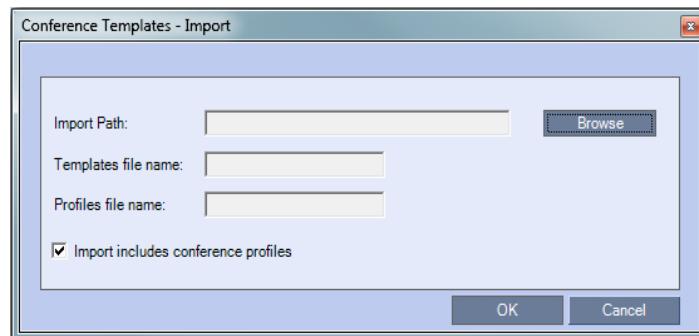
3   Optional. Clear the **Import includes conference profiles** check box when you only want to import *Conference Templates*.

When this check box is cleared, the *Conference Templates - Import* dialog box is displayed without the *Profiles file name* field.

Conference Templates - Import

Import Path:

Browse

Templates file name:

☐ Import includes conference profiles

OK   Cancel
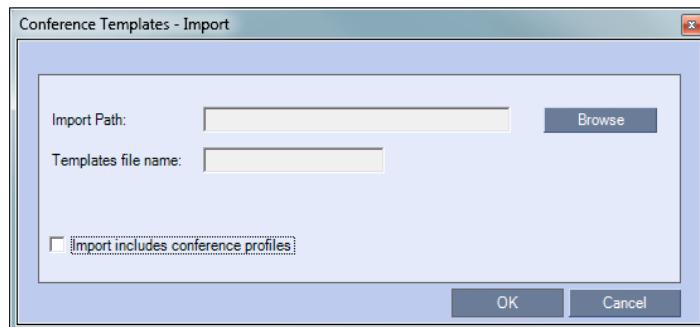
4   In the *Import Path* field, click **Browse** to navigate to the path and file name of the *Conference Templates* you want to import.

When clicking the exported templates file you want to import, the system automatically displays the appropriate files in the *Templates file name* field and the *Profiles file name* field (when the **Import includes conference profiles** check box is selected).

5   Click **OK** to import the *Conference Templates* and their associated *Conference Profiles*, if selected.

Conference Templates are not imported when:

— A *Conference Template* already exists

— An associated *Conference Profile* is not defined in the *Conference Profiles* list

When one or more *Conference Templates* are not imported, a Message Alert window is displayed with the templates that were not imported.

Current Message Number: 1

Jeff1_1546854610: Display name already exists

Back   Next   Cancel
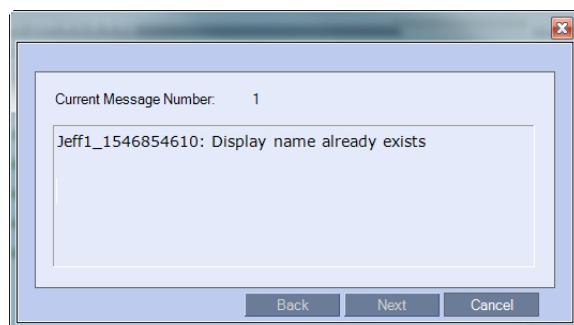
6   Click **Cancel** to exit the *Message Alerts* window.

The imported *Conference Templates* are added to the *Conference Templates* list. When the **Import includes conference profiles** check box is selected, the imported *Conference Profiles* are added to the *Conference Profiles* list.

12

Conference and Participant Monitoring

Viewing Permissions			
Tab	Chairperson	Operator	Administrator
Skins	✔	✔	✔
IVR		✔	✔
Info	✔	✔	✔

You can monitor ongoing conferences and perform various operations while conferences are running.

Three levels of monitoring are available with the Collaboration Server:

- *General Monitoring* - You can monitor the general status of all ongoing conferences and their participants in the main window.
- *Conference Level Monitoring* - You can view additional information regarding a specific conference and modify its parameters if required, using the *Conference Properties* option.
- *Participant Level Monitoring* - You can view detailed information on the participant's status, using the *Participant Properties* option.
- The maximum number of participants in a conference:
  — Polycom RMX 1800 with 3 video accelerators: Up to 100 HD 720p 30 or 50 HD 1080p 25/30 fps.
  — Polycom RMX 1800 with 2 video accelerators: Up to 70 HD 720p 30 or 35 HD 1080p 25/30 fps.
  — Polycom RMX 1800 with 1 video accelerators: Up to 35 HD 720p 30 or 17 HD 1080p 25/30 fps.

General Monitoring

Users can monitor a conference or keep track of its participants and progress. For more information, see *Polycom RMX 1800 Getting Started Guide*, *"Monitoring Ongoing Conferences"* on page **3-31**.
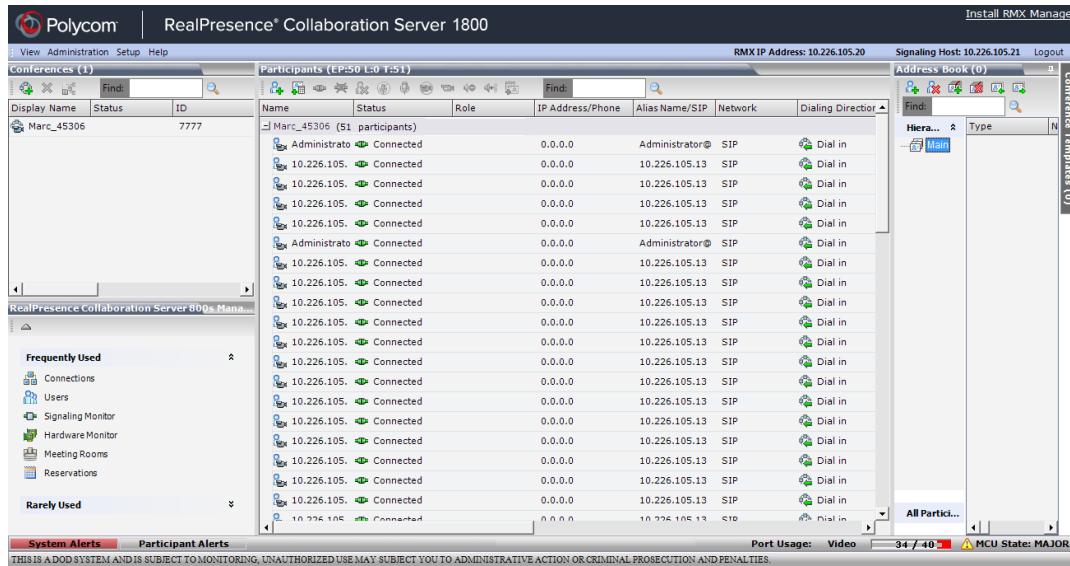
You can click the blinking **Participant Alerts** indication bar to view participants that require attention. For more information, see *"System and Participant Alerts"* on page **19-1**.

Conference Level Monitoring

In addition to the general conference information that is displayed in the *Conference* list pane, you can view the details of the conference's current status and setup parameters, using the *Conference Properties* dialog box.

Viewing the Properties of an Ongoing CP Conference

To view the parameters of an ongoing CP conference:

1   In the *Conference* list pane, double-click the **CP** conference or right-click the **CP** conference and then click **Conference Properties**.

The *Conference Properties - General* dialog box with the **General** tab opens.
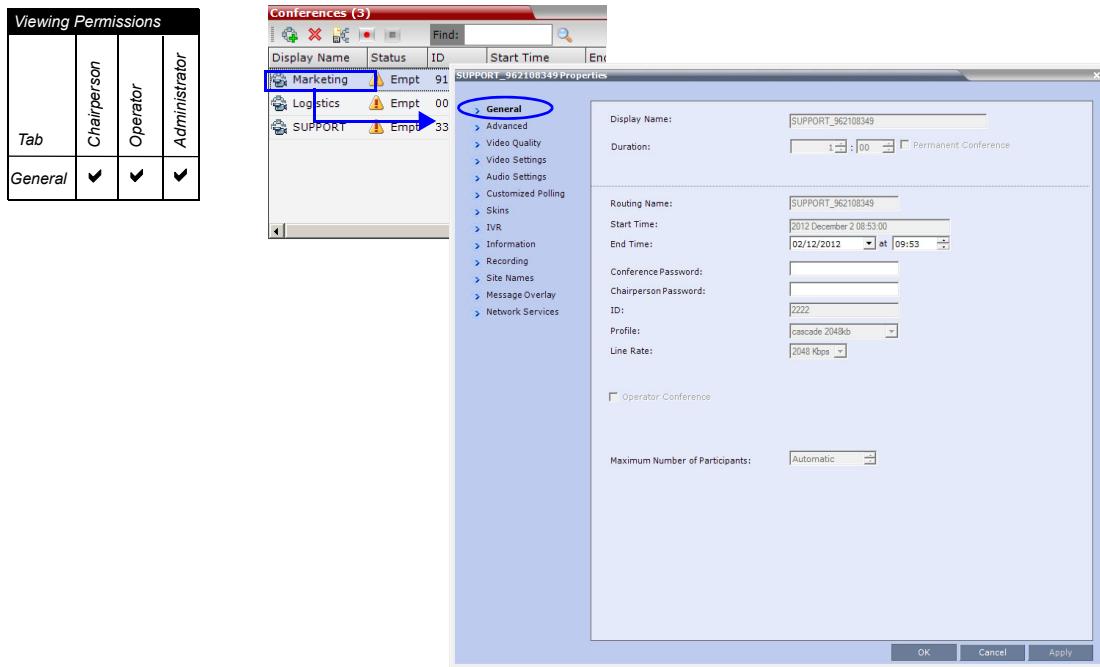
The following information is displayed in the *General* tab:

Table 12-1 Conference Properties - General

Field	Description
Display Name	The Display Name is the conference name in native language and Unicode character sets to be displayed in the *Collaboration Server Web Client*. **Note:** This field is displayed in all tabs.
Duration	The expected duration of the conference using the format HH:MM. **Note:** This field is displayed in all tabs.
Permanent Conference	Indicates whether the conference is set as a Permanent Conference, with no pre-determined End Time. This conference continues until it is terminated by an administrator, operator or chairperson. **Note:** This field is displayed in all tabs.
Routing Name	The ASCII name of the conference. It can be used by H.323 and SIP participants for dialing in directly to the conference. It is used to register the conference in the gatekeeper and the SIP server.
Start Time	The time the conference started.
End Time	The expected conference end time. **Note:** This field is not shown when the conference is set as a *Permanent Conference*.
Conference Password	A numeric password for participants to access the conference.

Table 12-1 Conference Properties - General (Continued)

Field	Description
Chairperson Password	A numeric password used by participants to identify themselves as the conference chairperson.
ID	The conference ID.
Profile	The name of the conference Profile from which conference parameters were taken.
Line Rate	The maximum transfer rate, in kilobytes per second (Kbps) of the call (video and audio streams).
Max Number of Participants	Indicates the total number of participants that can be connected to the conference. The Automatic setting indicates the maximum number of participants that can be connected to the MCU according to resource availability.

2 Click the **Advanced** tab.

The *Conference Properties - Advanced* dialog box opens.
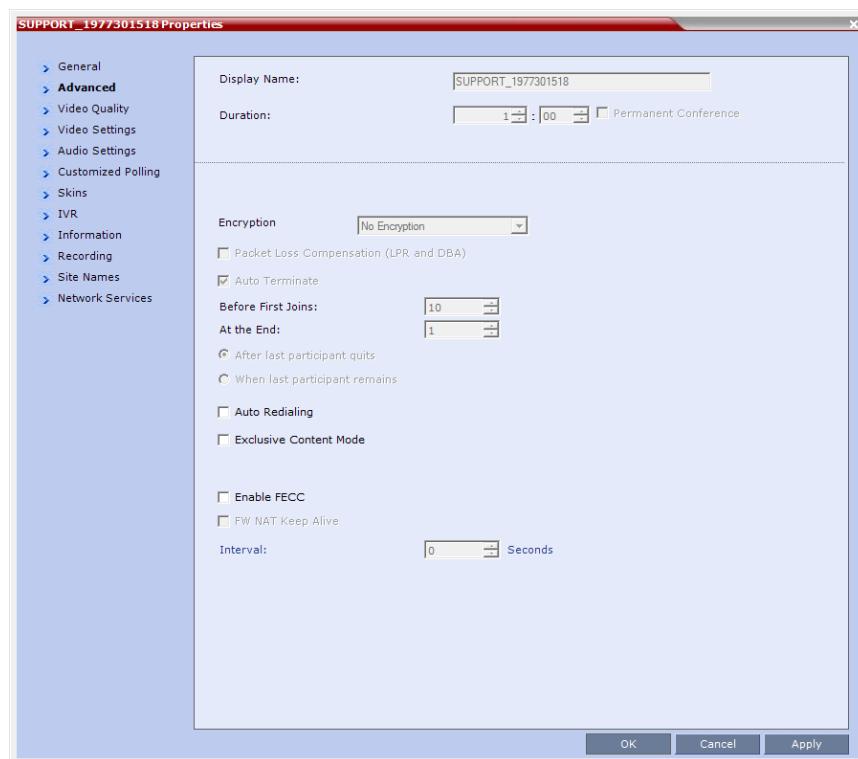
3 The following information is displayed in the *Advanced* tab:

Table 12-2 Conference Properties - Advanced Parameters

Field/Option	Description
Encryption	Indicates whether the conference is encrypted.

Table 12-2 Conference Properties - Advanced Parameters (Continued)

Field/Option	Description
Packet Loss Compensation (LPR and DBA)	Indicates wether Packet Loss Compensation (LPR and DBA) is enabled for the conference.
Auto Terminate	When selected, indicates that the MCU will automatically terminate the conference when *Before First Joins*, *At the End-After Last Quits and At the End - When Last Participant Remains* parameters apply.
Auto Redialing	Indicates whether dial-out participants are automatically (when selected) or manually (when cleared) connected to the conference.
Exclusive Content Mode	When selected, *Content* is limited to one participant.
Enable FECC	When selected, Far End Camera Control is enabled.
FW NAT Keep Alive	When selected, sends a *FW NAT Keep Alive* message at specific Intervals for the RTP, UDP and BFCP channels. The interval specifies how often a *FW NAT Keep Alive* message is sent. For more information, see

4 Click the **Video Quality** tab.

The *Conference Properties - Video Quality* dialog box opens.
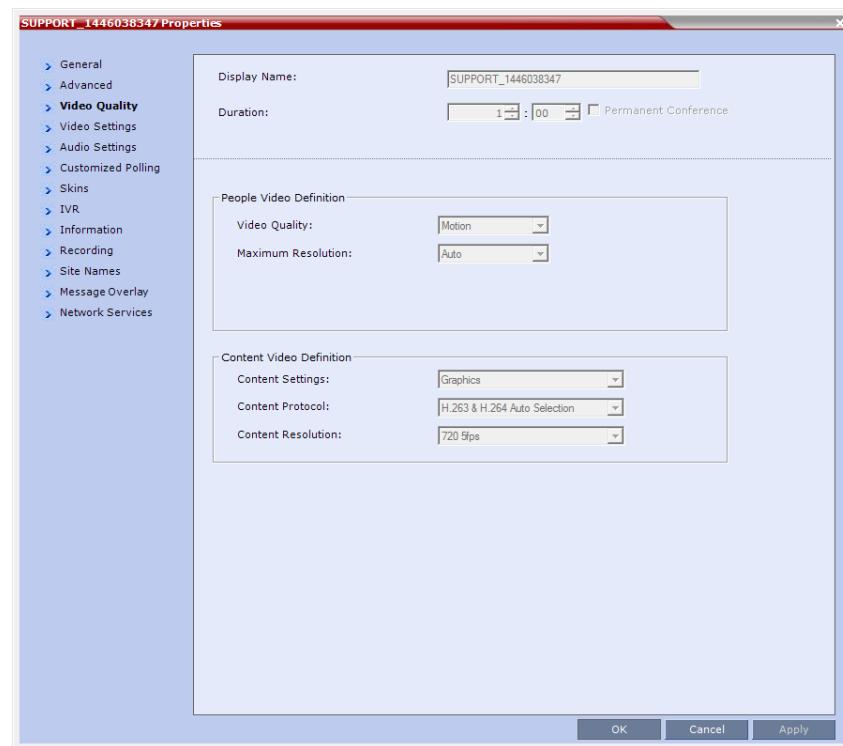
The following information is displayed:

Table 12-3 *Conference Properties - Video Quality Parameters*

Field/Option	Description
People Video Definition	
Video Quality	Indicates the resolution and frame rate that determine the video quality set for the conference. Possible settings are: **Motion** or **Sharpness**. For more information, see "*Video Resolutions in AVC-based CP Conferencing*" on page **4-1**.
Maximum Resolution	Indicates the *Maximum Resolution* setting for the conference. • *Auto* (default) - indicates that the *Maximum Resolution* is as selected in the *Resolution Configuration* dialog box. The *Maximum Resolution* settings for conferences and participants cannot be changed during an ongoing conference.
Content Video Definition	
AS-SIP	Indicates if AS-SIP is enabled for the conference. For more information, see "*Enabling AS-SIP Content*" on page **23-51**.
Multiple Content Resolutions	Indicates if *Multiple Content Resolutions* mode for content sharing is enabled.
Content Settings	Indicates the Content channel resolution set for the conference. Possible resolutions are: • **Graphics –** default modePolycom RMX 1800 • **Hi-res Graphics –** requiring a higher bit rate • **Live Video –** content channel is live video • **Customized Content Rate** - resolution is manually defined.
Content Protocol	Indicates the Content Protocol used for content sharing in Highest Common Content Sharing Mode. For more information, see "*Content Protocols*" on page **4-7**.
Content Resolution	Indicates the Content Resolution and frame rate according to the selected Content Sharing Mode (Highest common Content or Multiple Resolution Contents) and the video protocol. For more information, see "*Defining Content Sharing Parameters for a Conference*" on page **4-3**.
Send Content to Legacy Endpoints (CP only)	This Content Sharing option is not supported with Polycom RMX 1800.

5 Click the **Video Settings** tab to list the video parameters.

Tab	Chairperson	Operator	Administrator
Viewing Permissions			
Video Settings	✔	✔	✔
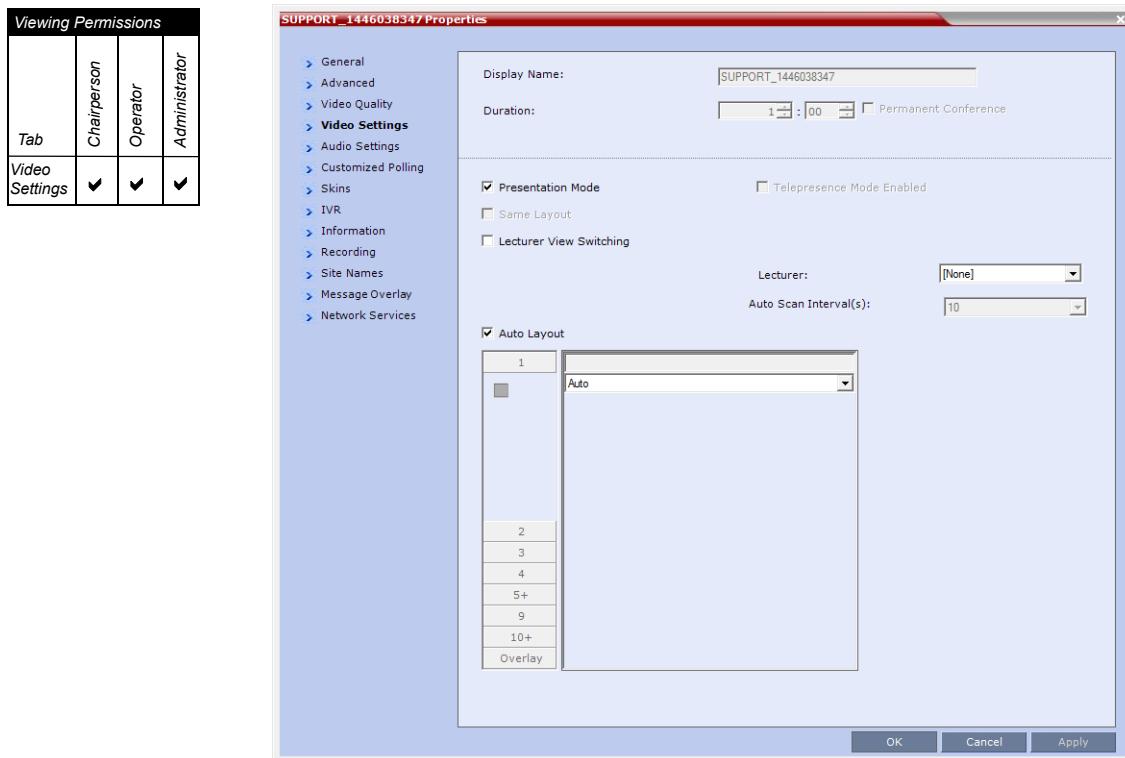
Table 12-4 Conference Properties - Video Settings Parameters

Field	Description
Presentation Mode	When checked, indicates that the Presentations Mode is active. For more information, see "*Presentation Mode*" on page **2-16**.
Lecturer View Switching	When checked, the *Lecturer View Switching* enables automatic random switching between the conference participants in the lecturer video window.
Same Layout	When checked, forces the selected layout on all conference participants, and the Personal Layout option is disabled.
Auto Layout	When enabled, the system automatically selects the conference layout based on the number of participants in the conference.
Lecturer	Indicates the name of the lecturer (if one is selected). Selecting a lecturer enables the Lecture Mode.
Auto Scan Interval(s)	The time interval, 10 - 300 seconds, that Auto Scan uses to cycle the display of participants that are not in the conference layout in the selected cell.

Table 12-4 Conference Properties - Video Settings Parameters (Continued)

Field	Description
Video Layouts (graphic)	Indicates the currently selected video layout.

6 Click the A**udio Settings** tab to view the audio setting for the conference.
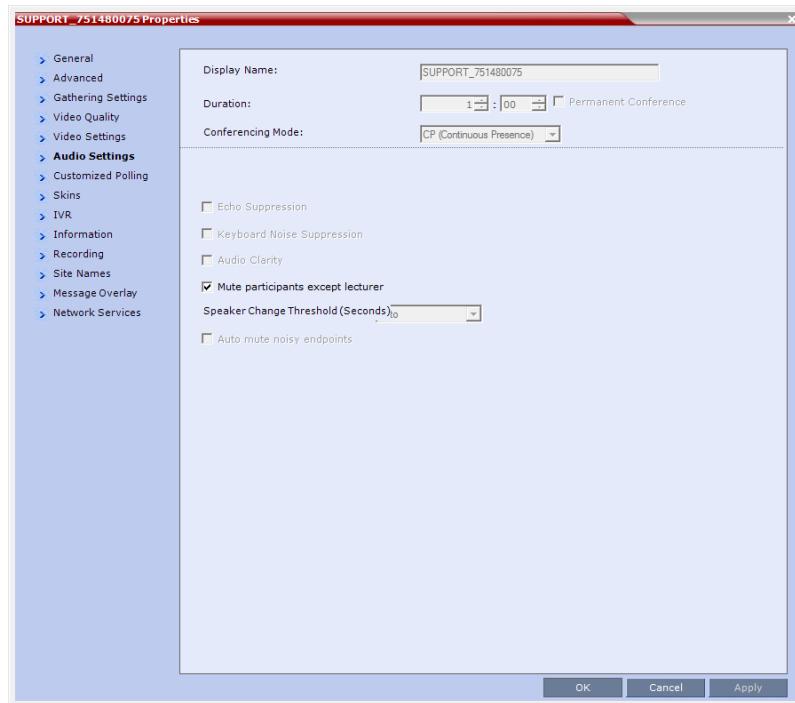
7 If needed, you can enable or disable the *Mute participants except lecturer* setting.

Click the **Customized Polling** tab to view and modify the customized polling for the conference.
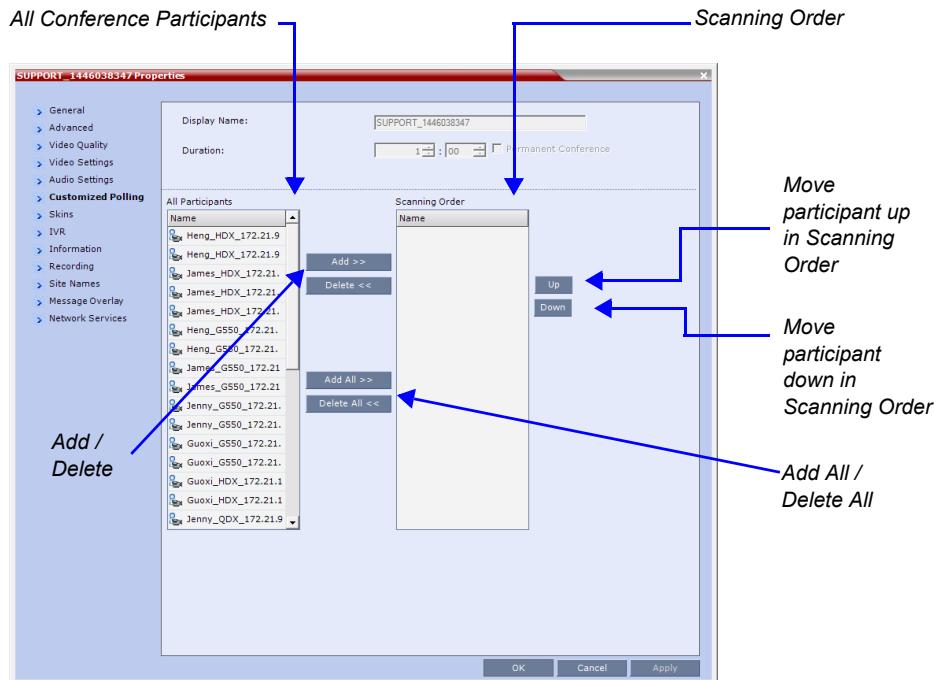
All conference participants are listed in the left pane (*All Participants*) while the participants that are to be displayed in the Auto Scan enabled cell of the video layout are listed in the right pane (*Scanning Order*).

The dialog box buttons are summarized in Table 12-5.

Table 12-5 *Customized Polling - Buttons*

Button	Description
Add	Select a participant and click this button to *Add* a the participant to the list of participants to be Auto Scanned. The participants name is removed from the *All Participants* pane.
Delete	Select a participant and click this button to *Delete* the participant from the list of participants to be *Auto Scanned*. The participants name is moved back to the *All Participants* pane.
Add All	Add all participants to the list of participants to be *Auto Scanned*. All participants' names are removed from the *All Participants* pane.
Delete All	Delete all participant from the list of participants to be *Auto Scanned*. All participants' names are moved back to the *All Participants* pane.
Up	Select a participant and click this button to move the participant *Up* in the *Scanning Order*.
Down	Select a participant and click this button to move the participant *Down* in the *Scanning Order*.

8 **Optional.** Add a participant to the list of participants to be *Auto Scanned*:

a Click on the participant's name in the *All Participants* list.

b Click the **Add** button to move the participant to the *Scanning Order* pane.

9 **Optional.** Delete a participant from the list of participants to be *Auto Scanned*:

a Click on a participant's name in the *Scanning Order* list.

b Click the **Delete** button to move the participant back to the *All Participants* pane.

10 **Optional.** Add all participants to the list of participants to be *Auto Scanned*:

— Click the **Add All** button.

11 **Optional.** Delete all participant from the list of participants to be *Auto Scanned*:

— Click the **Delete All** button.

12 **Optional.** Move the participant up in the *Scanning Order*:

— Click the **Up** button.

13 **Optional.** Move the participant down in the *Scanning Order*:

— Click the **Down** button.

14 Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open.

or

Click the **OK** the button to confirm and return to the *Collaboration Server Web Client Main Screen*.

15 Click the **Skins** tab to view the skin selected for the conference.

You cannot select another skin during an ongoing conference.

16 Click the **IVR** tab to view the IVR settings.

17 Click the **Information** tab to view general information defined for the conference. Changes made to this information once the conference is running are not saved to the CDR.

18 Click the **Recording** tab to review the recording settings for the conference.

19 Click the **Site Names** tab to enable or disable the display of site names during the conference, and adjust the display properties.

20 Click the **Message Overlay** tab to send text messages to the conference participants during the conference, and adjust the display properties of the text messages.
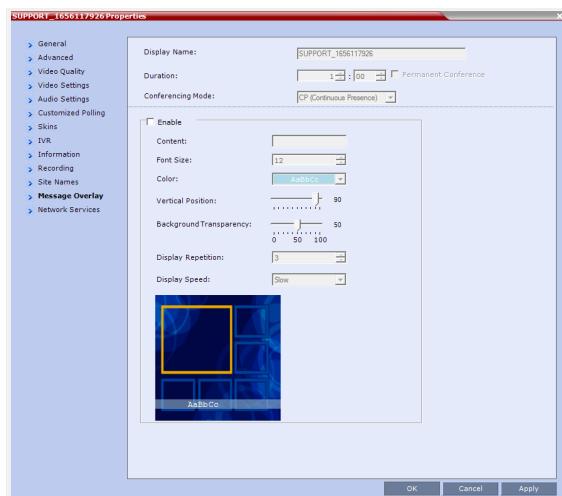
For more information, see "*Message Overlay for Text Messaging*" on page .

21 Click the **Network Services** tab to verify the SIP registration for the conference.

22 Click **OK** to close the *Conference Properties* dialog box.

23 Click the **Video Settings** tab to view the video parameters defined for the conference.
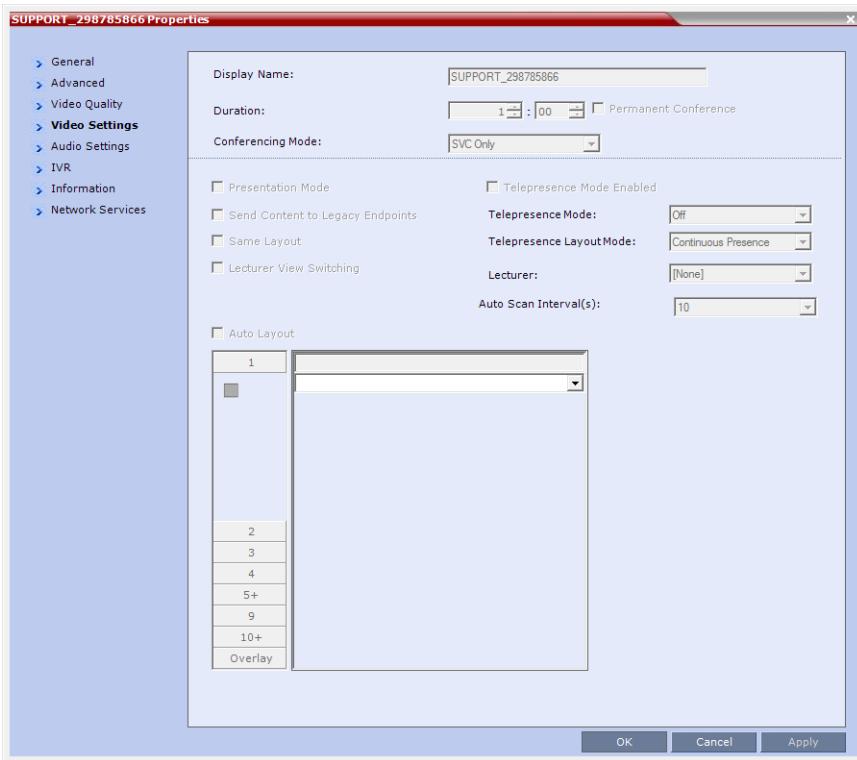
In SVC conferences, only Auto Layout is enabled and cannot be disabled. All other video settings are disabled.

24 Click the **Audio Settings** tab to view the audio parameters defined for the conference.
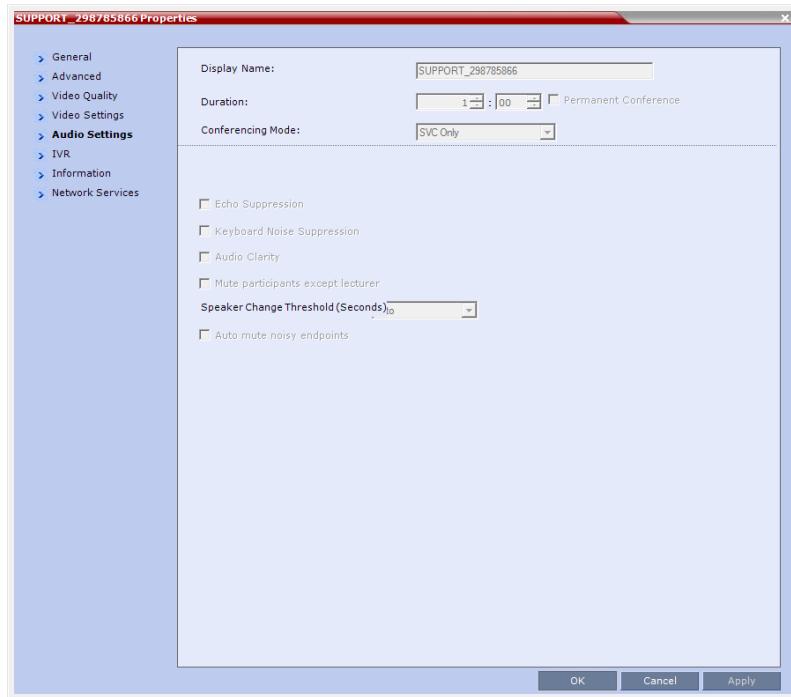
In SVC conferences, all Audio Settings options are disabled.

Monitoring Operator Conferences and Participants Requiring Assistance (CP Conferences)

Operator conferences are monitored in the same way as standard ongoing conferences.

Each Operator conference includes at least one participant - the Operator.

You can view the properties of the *Operator conference* by double-clicking the conference entry in the *Conferences* list or by right-clicking the conference entry and selecting **Conference Properties**. For more information, see the *Polycom RMX 1800 Getting Started Guide*, *"Conference Level Monitoring"* on page **3-32**.

Requesting Help

A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device. The participant can request *Individual Assistance* (default DTMF code ***0**) or *Conference Assistance* (default DTMF code **00**).

Participants in Entry Queues who failed to enter the correct destination conference ID or the conference password will wait for operator assistance (provided that an Operator conference is active).

When requiring or requesting operator assistance, the Collaboration Server management application displays the following:

- The participant's connection *Status* changes, reflecting the help request. For details, see Table 12-6.
- The conference status changes and it is displayed with the exclamation point icon and the status "Awaiting Operator".
- The appropriate voice message is played to the relevant participants indicating that assistance will be provided shortly.

The following icons and statuses are displayed in the *Participant Status* column:

Table 12-6   *Participants List Status Column Icons and Indications*

Icon	Status indication	Description
	Awaiting Individual Assistance	The participant has requested the operator's assistance for himself/herself.
	Awaiting Conference Assistance	The participant has requested the operator's assistance for the conference. Usually this means that the operator is requested to join the conference.

When the Operator moves the participant to the *Operator conference* for individual assistance the participant Status indications are cleared.

Request to Speak

Participants that were muted by the conference organizer/system operator can indicate that they want to be unmuted by entering the appropriate DTMF code.

An icon is displayed in the *Role* column of the *Participants* list for 30 seconds.

Request to Speak is:

- Activated when the participant enters the appropriate DTMF code (default: **99)**.

  The DTMF code can be modified in the conference *IVR Service Properties - DTMF Codes* dialog box.
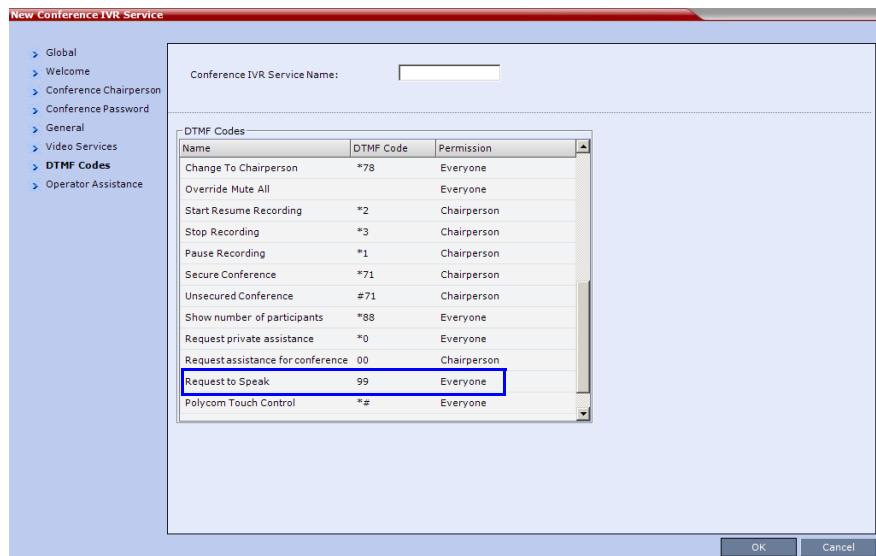
- Available for dial-in and dial-out participants.
- A participant can request to speak more than once during the conference.
- Supported in *all* conference types.
- Supported in H.323 and SIP environments.
- The duration of the icon display cannot be modified.

Participant Alerts List

The *Participant Alerts* list contains all the participants who are currently waiting for operator assistance.

Participants are automatically added to the *Participants Alerts* list in the following circumstances:

- The participant fails to connect to the conference by entering the wrong conference ID or conference password and waits for the operator's assistance.
- The participant requests Operator's Assistance during the ongoing conference.

This list is used as reference only. Participants can be assisted and moved to the *Operator conference* or the destination conference only from the *Participants* list of the Entry Queues or ongoing conference where they are awaiting assistance.

The participants are automatically removed from the *Participant Alerts* list when moved to any conference (including the *Operator conference*).

Participant Level Monitoring

In addition to conference information, you can view detailed information regarding the status and parameters of each listed participant, using the *Participant Properties* dialog box. Participant properties can be displayed for all participants currently connected to a conference and for defined participants that have been disconnected.

Displaying Participants Properties

To display the participant Properties:

1 In the *Participant List* pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

The *Participant Properties - Media Sources* dialog box opens.

Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Media Sources	✔	✔	✔

AVC-based Participant
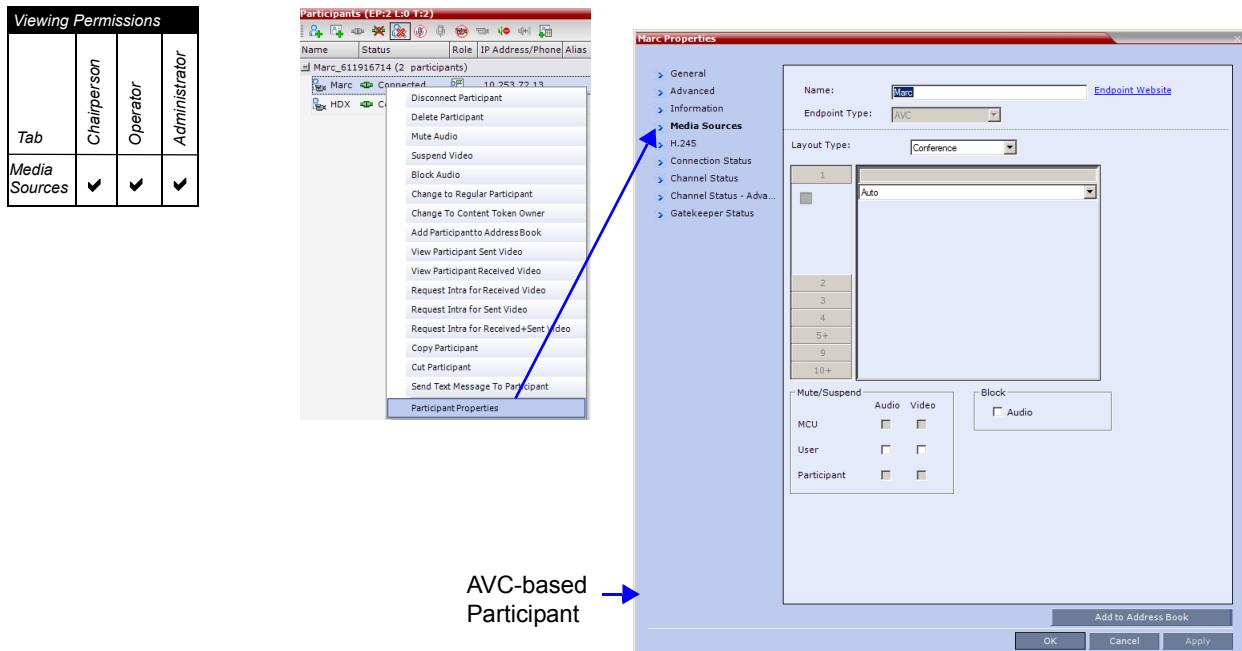
The *Media Sources* dialog box enables you to mute participant's audio, suspend participant's video transmission and select a personal Video Layout for the participant.

IP Participant Properties

The following parameters are displayed for an IP participant

Table 12-7   Participant Properties - Media Sources Parameters

Field	Description
Name	Indicates the participant's name. **Note:** This field is displayed in all tabs.

Table 12-7 Participant Properties - Media Sources Parameters (Continued)

Field	Description
Endpoint Website (link)	Click the Endpoint Website hyperlink to connect to the internal website of the participant's endpoint. It enables you to perform administrative, configuration and troubleshooting activities on the endpoint. The connection is available only if the IP address of the endpoint's internal site is filled in the *Website IP Address* field in the *Participant Properties - General* dialog box. **Note:** This field is displayed in all tabs**.**
Endpoint Type	Indicates whether the participant is using an AVC-based endpoint. **Note:** This field is displayed in all tabs.
Layout Type	Indicates whether the video layout currently viewed by the participant is the Conference or Personal Layout. If *Personal Layout* is selected, you can select a Video Layout that will be viewed only by this participant.
Video Layout	Indicates the video layout currently viewed by the participant. When *Personal Layout* is selected in the *Layout Type* you can force participants to the video windows in a layout that is specific to the participant. For more information*, see Polycom RMX 1800 Getting Started Guide,* "*Changing the Video Layout of a Conference"* on page **3-46**.
Mute/Suspend	Indicates if the endpoint's audio and/or video channels have been muted/suspended. The entity that initiated audio mute or video suspend is also indicated. • **MCU** – Audio or Video channel has been muted/suspended by the MCU. • **User** – Channels have been muted/suspended by the Collaboration Server user. • **Participant** – Channels have been muted/suspended by the participant from the endpoint. You can also cancel or perform mute and suspend operation using these check boxes. **Note:** If the participant muted his/her audio channel, the system displays the mute icon only for H.323. This icon is not displayed for SIP participant due to SIP standard limitation.
Block	When checked, the audio transmission from the conference to the participant's endpoint is blocked, but the participant will still be heard by other participants.

2 Click the **Connection Status** tab to view the connection status, and if disconnected the cause of the disconnection.

Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Connection Status	✔	✔	✔
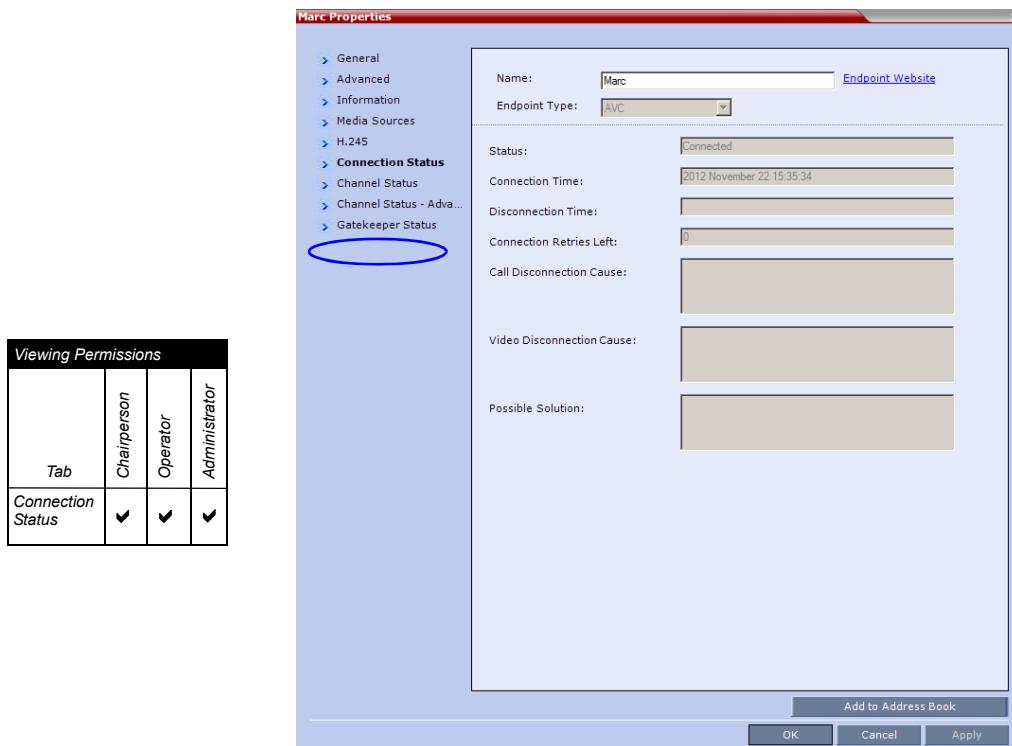
The following parameters are displayed:

Table 12-8 Participant Properties - Connection Status Parameters

Field	Description
Participant Status	
Status	Indicates the connection status of the participant.
Connection Time	The date and time the participant connected to the conference. **Note:** The time format is derived from the MCU's operating system time format.
Disconnection Time	The date and time the defined participant disconnected from the conference.
Connection Retries Left	Indicates the number of retries left for the system to connect defined participant to the conference.
Call Disconnection Cause	Displays the cause for the defined participant's disconnection from the conference. See *Appendix A:* "*Disconnection Causes*" on page **A-1**.
Video Disconnection Cause	Displays the cause the video channel could not be connected. For more information, see *Appendix A:* "*Disconnection Causes*" on page **A-1**.

Table 12-8 Participant Properties - Connection Status Parameters (Continued)

Field	Description
Possible Solution	In some cases, a possible solution is indicated to the cause of the video disconnection.

3 Click the **H.245** (H.323) or **SDP** (SIP) tab during or after the participant's connection process to view information that can help in resolving connection issues.

*LPR activity
(Displayed in all three panes)*

*Displays the endpoint's actual
capabilities used for the connection*

**H.323 Participant
(AVC-based|)**
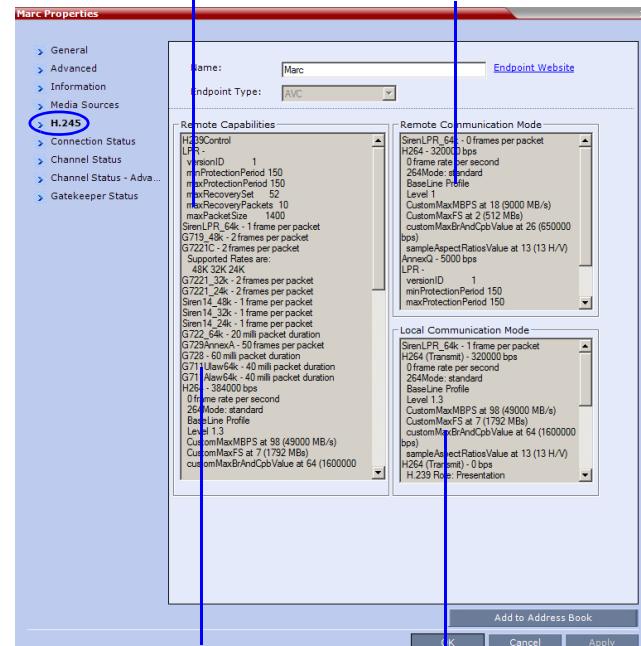
*List's the endpoint's capabilities as
retrieved from the remote site*

*Displays the MCU's capabilities used for
connection with the participant*
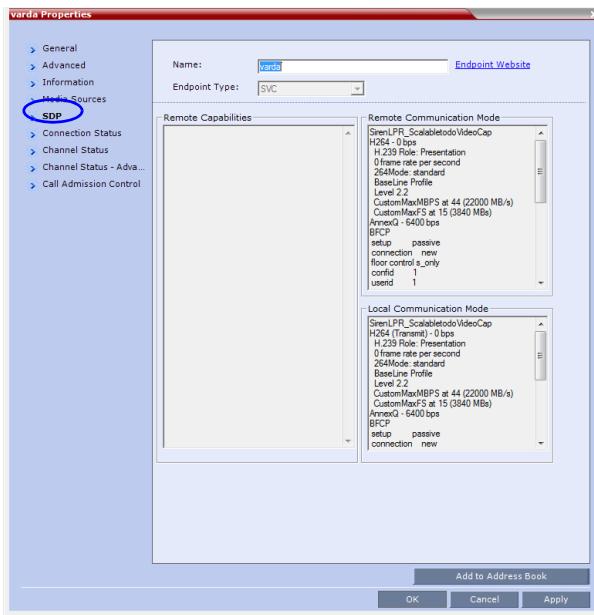
SIP Participant (AVC-based)

Table 12-9 *Participant Properties - H.245/SDP Parameters*

Field	Description
Remote Capabilities	Lists the participant's capabilities as declared by the endpoint.
Remote Communication Mode	Displays the actual capabilities used by the endpoint when establishing the connection with the MCU (Endpoint to MCU).
Local Communication Mode	Displays the actual capabilities used by the MCU when establishing the connection with the participant's endpoint (MCU to Endpoint).

4 Click on the **Channel Status** tab to view the status of the various channels.

Tab	*Chairperson*	*Operator*	*Administrator*
Channel Status		✔	✔

Viewing Permissions

Marc Properties

> General
> Advanced
> Information
> Media Sources
> H.245
> Connection Status
> **Channel Status**
> Channel Status - Adva...
> Gatekeeper Status

Name: Marc   Endpoint Website
Endpoint Type: AVC

Channels Used:

Channel	Faulty	Bit Rate	Packet Loss	Fraction Loss
☑ H.225				
☑ H.245				
☑ Audio in		64.0	0	0.00%(0.00%
☑ Audio out		64.0	0	0.00%(0.00%
☑ Video in		5.7	0	0.00%(0.00%
☑ Video out		264.6	0	0.00%(0.00%

Sync Status:

Channel	Source	Position	Protocol Sync Loss	Video Intra S
Video	HDX 4000 TW	■	0	

	Rate	Video Sync Loss	LPR activation
Tx	384000	(1)	
Rx	384000	(0)	

☐ FECC Token   ☐ Content Token

Add to Address Book

OK   Cancel   Apply

The following parameters are displayed:

Table 12-10 *Participant Properties - Channel Status Parameters*

Field	Description
Channels Used	When checked, indicates the channel type used by the participant to connect to the conference: Incoming channels are endpoint to MCU, Outgoing channels are from MCU to endpoint. **Channels:** • *H.225/Signaling* - The call-signaling channel. • *H.245/SDP* - The Control channel. • *Audio in - Incoming audio channel* • *Audio out - Outgoing audio channel* • *Video in - Incoming video channel* • *Video out - Outgoing video channel* • *Content in* - H.239/People+Content conferences • *Content out* - H.239/People+Content conferences • *FECC in* - The incoming FECC channel is open. • *FECC out* - The outgoing FECC channel is open. **Columns:** • **Faulty** – A red exclamation point indicates a faulty channel condition. This is a real-time indication; when resolved the indication disappears. An exclamation point indicates that further investigation may be required using additional parameters displayed in the *Advanced Channel Status* tab. • **Bit Rate** – The actual transfer rate for the channel. When channel is inactive, bit rate value is 0. For example, if the participant is connected without video, the bit rate for the video channel is 0. **Note:** The CTS Audio Auxiliary channel is used only for Content. In all other cases, the bit rate shown in this column for this channel is 0. • **Packet Loss** – The accumulated count of all packets that are missing according to the RTCP report since the channel was opened. This field is relevant only during the connection stage and does not display faulty indications. • **Fraction Loss (Peak)** – The ratio between the number of lost packets and the total number of transmitted packets since the last RTCP report. *Peak* (in parentheses) indicates the highest ratio recorded since the channel was opened. • **Number of Packets** – The number of received or transmitted packets since the channel has opened. This field does not cause the display of the faulty indicator. • **Jitter (Peak)** – Displays the network jitter (the deviation in time between the packets) as reported in the last RTCP report (in milliseconds). *Peak* (in parentheses) reflects the maximum network jitter since the channel was opened. • **Latency** – Indicates the time it takes a packet to travel from one end to another in milliseconds (derived from the RTCP report). High latency value may indicate that there is a problem in the network, or that the endpoint is sending an incorrect RTCP values.

Table 12-10 Participant Properties - Channel Status Parameters (Continued)

Field	Description
Sync Status	*Channel* - The channel type: Video or Content. *Source* - The name of the participant currently viewed by this participant. **Position** - The video layout position indicating the place of each participant as they appear in a conference. **Protocol Sync Loss** - Indicates whether the system was able to synchronize the bits order according to the selected video protocol. **Video Intra Sync** - Indicates whether the synchronization on a video Intra frame was successful. **Video Resolution** - The video resolution of the participant.
Rx - Rate	The received line rate.
Tx - Rate	The transmitted line rate.
Tx - Video Sync Loss	When checked, indicates a video synchronization problem in the outgoing channel from the MCU. The counter indicates the sync-loss count.
Rx - Video Sync Loss	When checked, indicates a video synchronization problem in the incoming channel from the endpoint. The counter indicates the sync-loss count.
Tx - LPR Activation	When checked, indicates LPR activation in the outgoing channel.
Rx - LPR Activation	When checked, indicates LPR activation in the incoming channel.
FECC Token	When checked, indicates that the participant is the holder of the FECC Token.
Content Token	When checked, indicates that the participant is the holder of the Content Token.

5   Click the **Channel Status Advanced** tab to view additional information for selected audio and video channels.

In the *Channel Status - Advanced* tab, channels can be selected for viewing additional information:
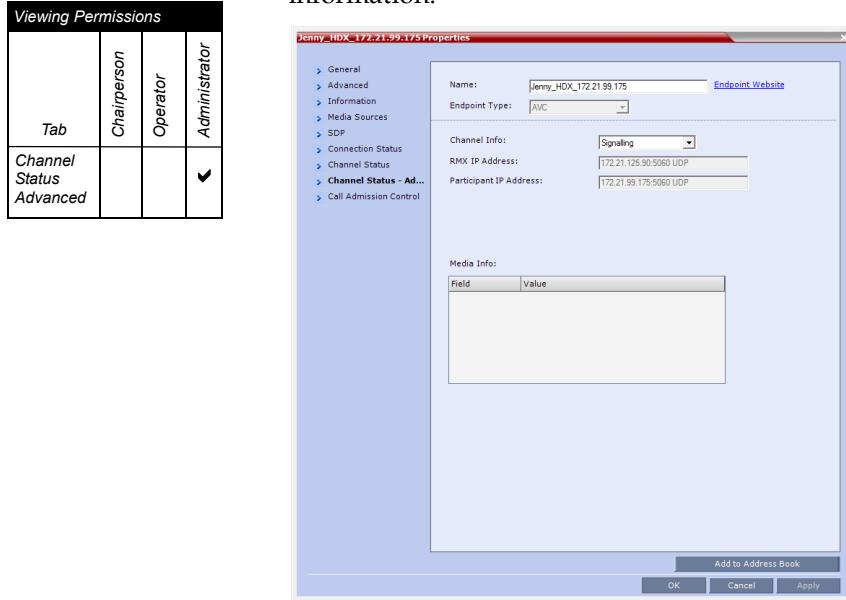
Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Channel Status Advanced			✔

Table 12-11 Participant Properties - Channel Status Advanced Parameters

Field	Description
Channel Info	Select a channel to view its information: • Signaling • Audio in • Audio out • Video in • Video out • Content in • Content Out • SIP BFCP TCP
RMX IP Address	The IP address and the transport protocol (TCP/UDP) of the MCU to which the participant is connected and the port number allocated to the participant incoming media stream on the MCU side.
Participant IP Address	The IP address and the transport protocol (TCP/UDP) of the participant and the port number allocated to the media stream on the participant side.
Media Info	This table provides information about the audio and video parameters, such as video algorithm, resolution, etc. For more information, see *Appendix E: "Participant Properties Advanced Channel Information"* on page **E-1**.

Table 12-11 Participant Properties - Channel Status Advanced Parameters (Continued)

Field	Description
RTP Statistics	This information may indicate problems with the network which can affect the audio and video quality. For more information, see *Appendix E:* "*Participant Properties Advanced Channel Information"* on page **E-1**.

6 **Optional for H.323 AVC-based participants.** Click the **Gatekeeper Status** tab to view its parameters.
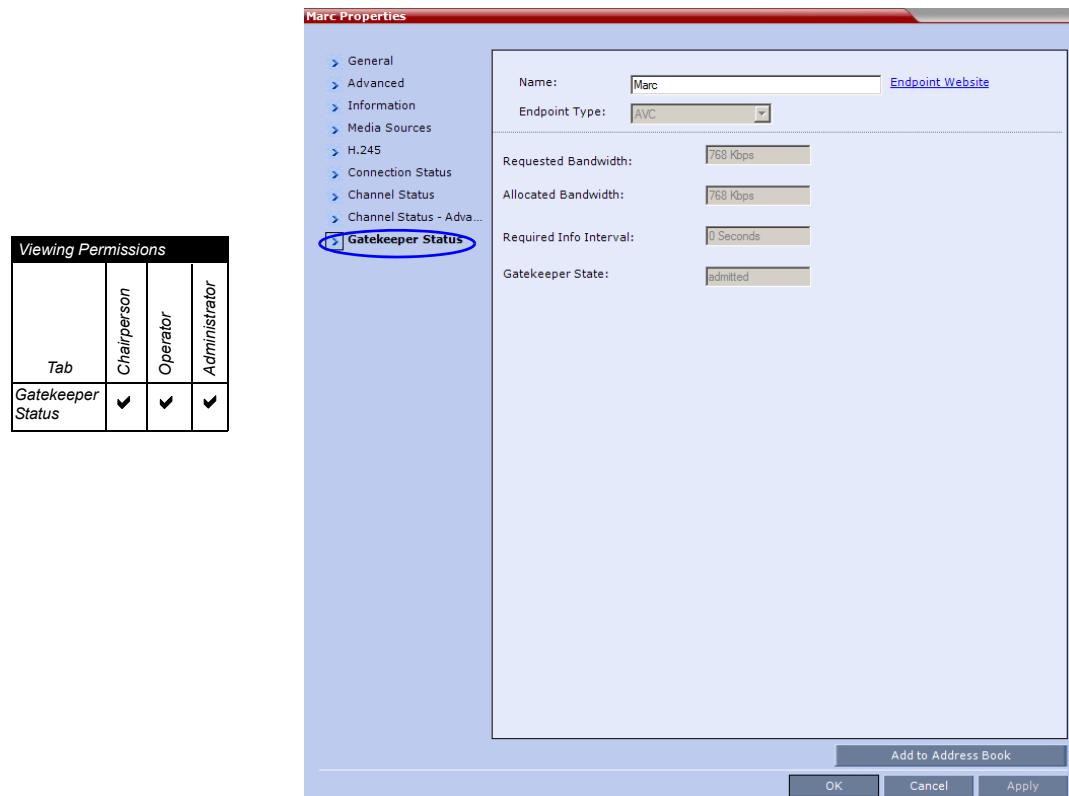
Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Gatekeeper Status	✔	✔	✔

Table 12-12 Participant Properties - Gatekeeper Status Parameters

Field	Description
Requested Bandwidth	The bandwidth requested by the MCU from the gatekeeper.
Allocated Bandwidth	The actual bandwidth allocated by the gatekeeper to the MCU.
Required Info Interval	Indicates the interval, in seconds, between registration messages that the MCU sends to the gatekeeper to indicate that it is still connected.

Table 12-12 Participant Properties - Gatekeeper Status Parameters (Continued)

Field	Description
Gatekeeper State	Indicates the status of the participant's registration with the gatekeeper and the bandwidth allocated to the participant. The following statuses may be displayed: • **ARQ** – Admission Request - indicates that the participant has requested the gatekeeper to allocate the required bandwidth on the LAN. • **Admitted** – indicates that the gatekeeper has allocated the required bandwidth to the participant. • **DRQ** – Disengage Request – the endpoint informs the gatekeeper that the connection to the conference is terminated and requests to disconnect the call and free the resources. • **None** – indicates that there is no connection to the gatekeeper.

7 **Optional for SIP AVC-based participants.** Click the **Call Admission Control** tab to view its parameters.
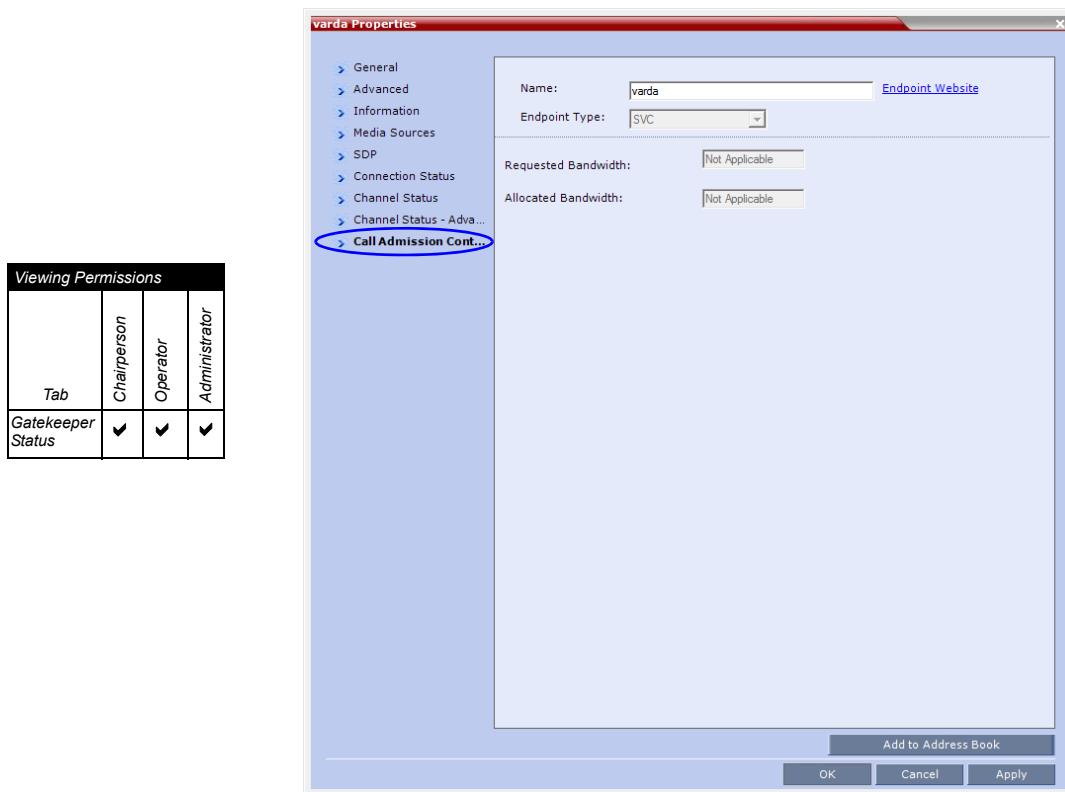
Viewing Permissions			
Tab	Chairperson	Operator	Administrator
Gatekeeper Status	✔	✔	✔

Table 12-13 Participant Properties - Gatekeeper Status Parameters

Field	Description
Requested Bandwidth	The bandwidth requested by the MCU from the SIP server.

Table 12-13 Participant Properties - Gatekeeper Status Parameters (Continued)

Field	Description
Allocated Bandwidth	The actual bandwidth allocated by the SIP server to the MCU.

Monitoring SIP BFCP Content

In the SIP *Participant Properties* dialog box, *BFCP* status information appears in:

• All three panes of the *SDP* tab.

• The *Channel Status* tab.

• The *Channel Status -Advanced* tab.

SDP

Channel Status

Channel Status - Advanced
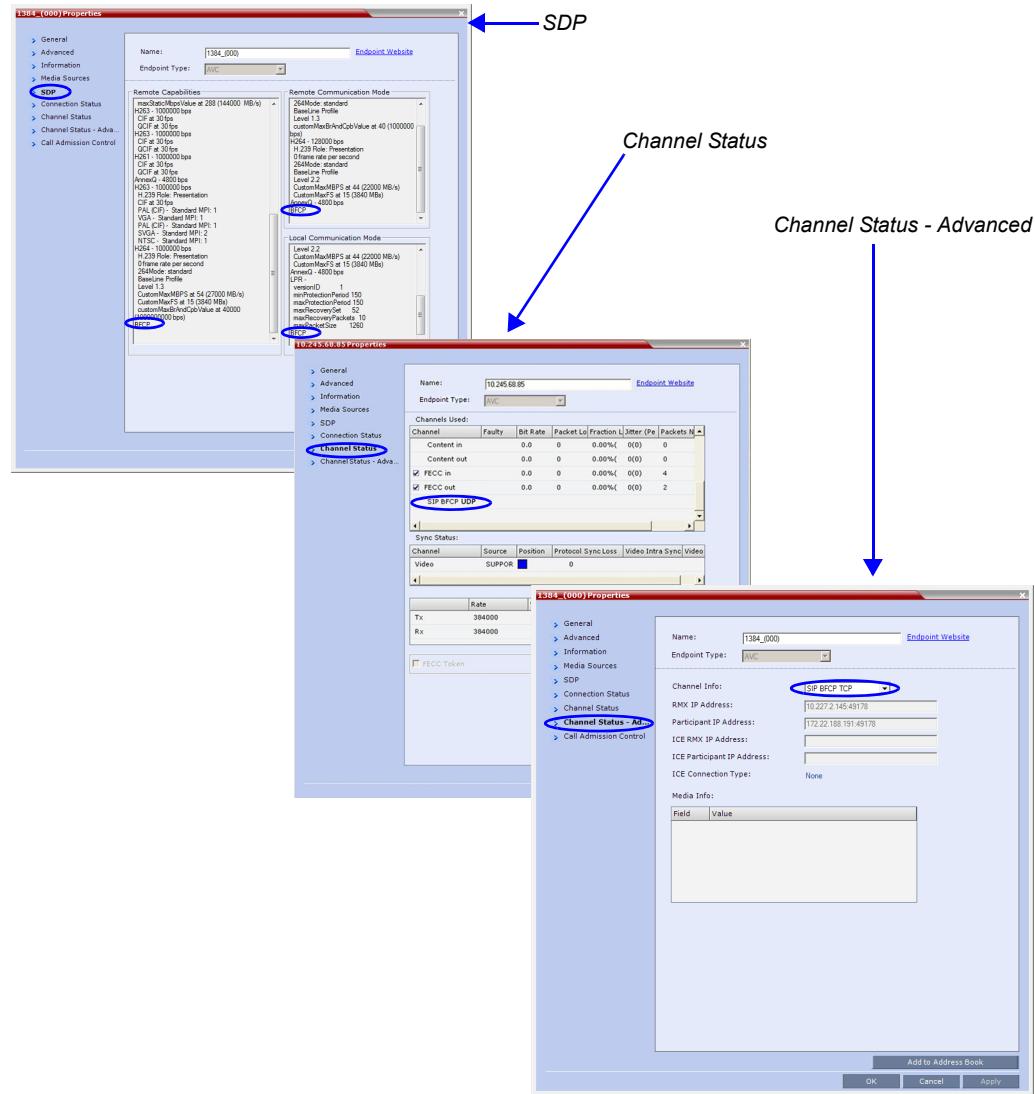
For more information see "*Participant Level Monitoring"* on page **12-15**.

Detecting SIP Endpoint Disconnection

When an abnormal disconnection of SIP endpoints occurs because of network problems or client application failures, SIP endpoints remain connected to the conference causing connection disruptions. For example, the video freezes in the layout or blocks content for SIP endpoints when a quick re-connection is performed. It can take several minutes to detect the SIP endpoint disconnection using the SIP standard behavior.

In a normal SIP video call, audio and video (RTP and RTCP) messages are sent from the endpoints to the MCU to detect the signaling of connected endpoints. Conversely, SVC endpoints might not send video RTP messages to the MCU when a participant is not displayed in the video layout of any of the participants in the conference. For SVC endpoints, the MCU will only verify audio RTP and RTCP messages and video RTCP messages. Video RTP messages will not be checked.

To detect the disconnection of SIP endpoints in a reasonable amount of time, a new system flag can be defined to specify the amount of time that the MCU should wait for an RTCP or RTP message from the SIP endpoint before the endpoint starts the disconnection process. The system default value is automatically set to 20 seconds.

The system flag, DETECT_SIP_EP_DISCONNECT _TIMER, contains the amount of time in seconds to wait for an RTCP or RTP message to be received from the endpoint. When the time that was set in the system flag has elapsed and no RTCP or RTP audio or video message has been received on either the audio or the video channel, the MCU disconnects the SIP endpoint from the conference. A CDR event record is created with a Call Disconnection Cause of "SIP remote stopped responding".

The Microsoft Lync add-in endpoint opens audio and content channels. Lync endpoints can send RTCP/RTP messages and empty RTP audio messages. When the time that was set in the system flag has elapsed and no RTCP or RTP message has been received on the audio channel, the MCU disconnects the endpoint from the conference.

SIP audio only endpoints use the audio channel only. When the time that was set in the system flag has elapsed and no RTCP or RTP message has been received on the audio channel, the MCU disconnects the SIP audio endpoint from the conference.

Configuring the System Flag

When you want to change the system default value of 20 seconds, the system flag, DETECT_SIP_EP_DISCONNECT_TIMER, can be manually added to the *System Flags* configuration to detect the disconnection of SIP endpoints. For more information see

The value range is from 0 to 300 seconds. When the value is set between 0 and 14, the feature is disabled and SIP endpoints are not detected for disconnection. When the value is set between 15 and 300, the feature is enabled.

13

Recording Conferences

Conferences running on the *Collaboration Server* can be recorded using a *Polycom® RSS™ Recording and Streaming Server* (*RSS*).

The recording system can be installed at the same site as the conferencing *MCU* or at a remote site. Several *MCU's* can share the same recording system.

Recording conferences is enabled via a *Recording Link*, which is a dial-out connection from the conference to the recording system.

Recording can start automatically, when the first participant connects to a conference, or on request, when the *Collaboration Server* user or conference chairperson initiates it.

Multiple Recording Links may be defined.

Each *Recording Link* defined on the *Collaboration Server* can be given a descriptive name and can be associated with one *VRR* saved on the *Polycom RSS 4000*.

The following guidelines apply:

*   A *Recording Link* that is being used by an ongoing conference cannot be deleted.
*   A *Recording Link* that is assigned to a *Profile* cannot be deleted.
*   While a *Profile* is being used in an ongoing conference, it cannot have a different *Recording Link* assigned to it.
*   Up to 100 Recording Links can be listed for selection in the Conference Profile.
*   *Multiple Recording Links* are supported in *Continuous Presence* and *Video Switched* conferences.
*   The number of *Recording Links* available for selection is determined by the value of the **MAXIMUM_RECORDING_LINKS** *System Flag* in *system.cfg*. Default value is 20 Recording Links.
*   The recording link can be encrypted when recording from an encrypted conference to the RSS that is set to encryption. For more details, see *"Recording Link Encryption"* on page **13-7**.

Creating Multiple Virtual Recording Rooms on the RSS

If the environment includes a *Polycom® RSS™ 4000 Version 8.5 Recording and Streaming Server (RSS)* and you want to associate *Recording Links* on the *Collaboration Server* with *Virtual Recording Rooms* (*VRR*), created and saved on the *Polycom® RSS™ 4000 Version 8.5* perform the following operations on the *RSS*:

1 Modify the parameters of a recording *Template* to meet the recording requirements.

2 Assign the modified recording *Template* to a *VRR*. The recording and streaming server will assign a number to the *VRR*.

3 Repeat Step 1 and Step 2 for each *VRR* to create additional *VRR*s.

For more information see the *RSS 4000 User Guide.*

Configuring the Collaboration Server to Enable Recording

To make recording possible the following components you must be configured on the *Collaboration Server*:

- *Recording Link* – defines the connection between the conference and the recording system.

- *Recording-enabled Conference IVR Service* – recording *DTMF* codes and messages must be set in the *Conference IVR* Service to enable "recording-related" voice messages to be played and to allow the conference chairperson to control the recording process using *DTMF* codes.

- *Recording-enabled Profile* – recording must be enabled in the *Conference Profile* assigned to the recorded conference.

If *Multiple Recording Links* are being defined for *Virtual Recording Rooms* (*VRRs*), created and saved on the *Polycom® RSS™ 4000 Version 8.5*, the **MAXIMUM_RECORDING_LINKS** *System Flag* in *system.cfg* can be modified to determine the number of *Recording Links* available for selection.

- **Range:** 20 - 100
- **Default:** 20

The flag value can be modified by selecting the *System Configuration* option from the *Setup* menu. For more information, see "*Modifying System Flags*" on page **20-1**.

Defining the Recording Link

The *Recording Link* is defined once and can be updated when the *H.323* alias or the IP address (of the recording system) is changed. Only one *Recording Link* can be defined in the *Collaboration Server*. Its type must be *H.323*.

> In *Multiple Networks* Configuration, Recording Links use the default Network Service to connect to conferences, therefore the recording system must be defined on the default IP Network Service to enable the recording.

To define a Recording Link:

1 In the *Collaboration Server Management* pane, click **Recording Links** (⚙️).

2 In the *Recording Links* list, click the **New Recording Link** (⚙️) button.

The *New Recording Link* dialog box is displayed.
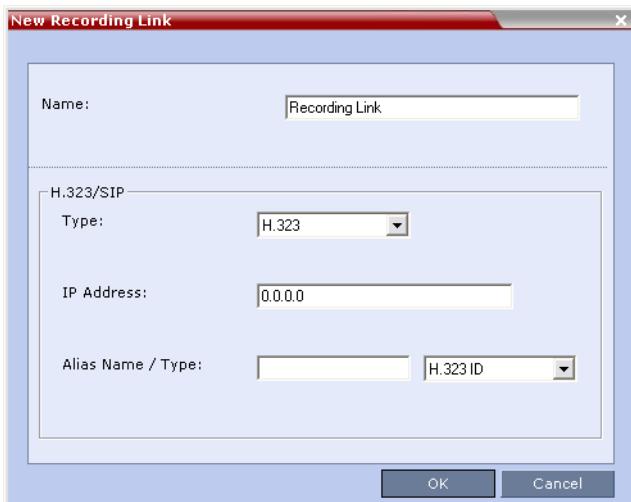
3 Define the following parameters:

Table 13-1 Recording Link Parameters

Parameter	Description
Name	Displays the default name that is assigned to the Recording Link. If multiple Recording Links are defined, it is recommended to use a descriptive name to be indicate the VRR to which it will be associated. Default: *Recording Link*
Type	Select the network environment: • H.323 • SIP
IP Address	• If no gatekeeper is configured, enter the IP Address of the RSS. Example: If the RSS IP address is 173.26.120.2 enter `173.26.120.2.` • If a gatekeeper is configured, you can either enter the IP address or an alias (see the alias description).
Alias Name	If using the endpoint's alias instead of IP address, first select the alias type and then enter the endpoint's alias. If you are associating this recording link to a VRR on the RSS, define the alias as follows: • If you are using the RSS IP address, enter the VRR number in the Alias field. For example, if the VRR number is 5555, enter **5555**. • Alternatively, if the *Alias Type* is set to **H.323 ID**, enter the RSS IP address and the VRR number in the format: **<RSS_IP_Address>##<VRR number>** For example: If the RSS IP is 173.26.120.2 and the VRR number is 5555, enter **173.26.120.2##5555**
Alias Type	Depending on the format used to enter the information in the IP address and Alias fields, select **H.323 ID** or **E.164** (for multiple Recording links). **E-mail ID** and **Participant Number** are also available.

4   Click **OK**.

The Recording Link is added to the *Collaboration Server* unit.

Enabling the Recording Features in a Conference IVR Service

To record a conference, a *Conference IVR Service* in which the recording messages and DTMF codes are activated must be assigned to the conference. The default *Conference IVR Service* shipped with the *Collaboration Server* includes the recording-related voice messages and default DTMF codes that enable the conference chairperson to control the recording process from the endpoint. You can modify these default settings.

To modify the default recording settings for an existing Conference IVR Service:

1   In the *Collaboration Server Management* pane, click the **IVR Services** (⊞) button.

The IVR Services are listed in the *IVR Services* list pane.

2   To modify the default recording settings, double-click the Conference IVR Service or right-click and select **Properties**.

The *Conference IVR Service Properties* dialog box is displayed.

3   To assign voice messages other than the default, click the **General** tab and scroll down the list of messages to the recording messages.
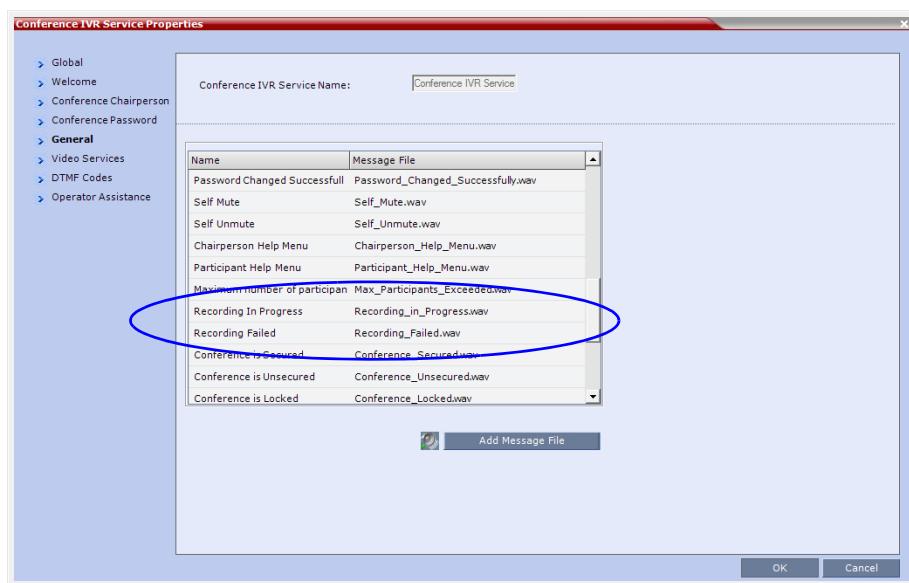
4   Select the *Recording In Progress* message, and then select the appropriate message file (by default, Recording_in_Progress.wav) from the file list to the right of the field.

5   Select the *Recording Failed* message, and then select the appropriate message file (by default, Recording_Failed.wav) from the file list to the right of the field.

6   To modify the default DTMF codes, click the **DTMF Codes** tab.

7   To modify the DTMF code or permission for a recording function:

   a   Select the desired DTMF name (Start, Stop or Pause Recording), click the DTMF code entry and type a new code.

Table 13-2   *Default DTMF Codes assigned to the recording process*

Recording Operation	DTMF Code	Permission
Start or Resume Recording	***3**	Chairperson
Stop Recording	***2**	Chairperson
Pause Recording	***1**	Chairperson

   b   In the *Permission* entry, select whether this function can be used by all conference participants or only the chairperson.

8   Click **OK**.

Enabling the Recording in the Conference Profile

To be able to record a conference, the recording options must be enabled in the *Conference Profile* assigned to it. You can add recording to existing *Profiles* by modifying them.

To enable recording for a conference:

1   In the *Collaboration Server Management* pane, click the **Conference Profiles** (🗂) button.

   The *Conference Profiles* list is displayed.

2   Create a new profile by clicking the **New Profile** (🗂) button or modify an existing profile by double-clicking or right-clicking an existing profile and then selecting **Profile Properties**.

> If creating a new profile, complete the conference definition. For more information on creating Profiles see on "*Defining New Profiles"* on page **2-9**.

3   In the *Profile Properties* dialog box, click the **Recording** tab.

4 Select the **Enable Recording** check box.
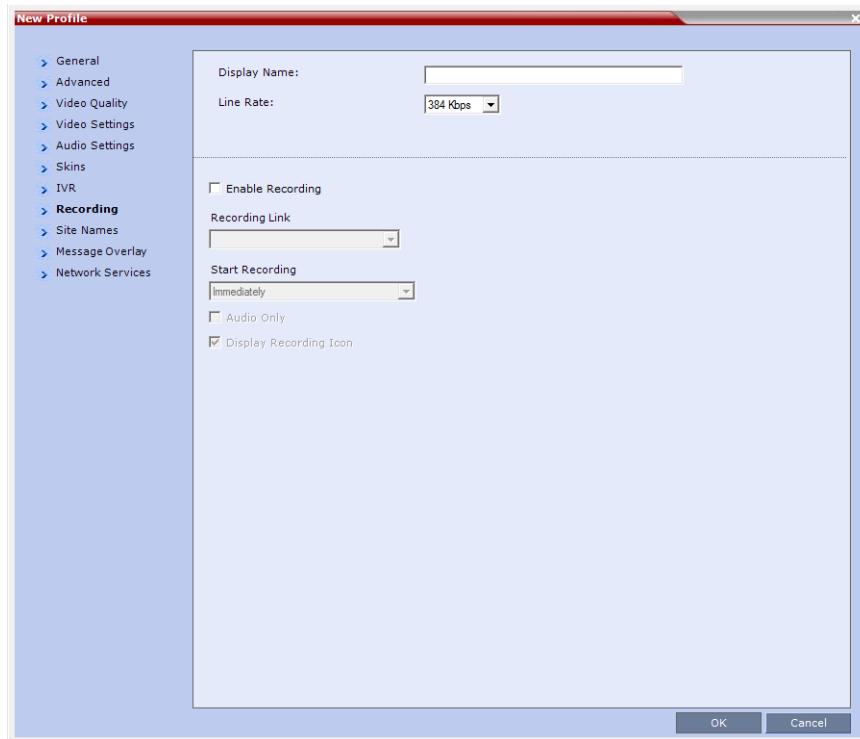
5 Define the following parameters:

Table 13-3 *Conference Profile Recording Parameters*

Parameter	Description
Enable Recording	Select to enable Recording Settings in the dialog box.
Recording Link	Select a recording link for the conference from the list.
Start recording	Select one of the following: • **Immediately** – conference recording is automatically started upon connection of the first participant. • **Upon Request** – the operator or chairperson must initiate the recording (manual).
Audio only	Select this option to record only the audio channel of the conference. **Note:** An *Audio Only* Recording Link cannot be used to record a conference if there are no Voice resources allocated in the *Video/Voice Port Configuration*.
Display Recording Icon	Select this option to display *Recording Indication* to all conference participants informing them that the conference is being recorded. The recording icon is replaced by a *Paused* icon when conference recording is paused.

6 Click **OK**.
Recording is enabled in the *Conference Profile*.

Recording Link Encryption

The Recording Link can be encrypted when recording an encrypted conference. The encryption of the *Recording Link* is enabled when *Encryption* is selected in the *Conference Profile* on the *Collaboration Server* and on the RSS, and the system flag **ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF** is set to **NO**.

Recording Link Encryption Guidelines:

*   The *Recording Link* connection type must be H.323.
*   The *Recording Link* uses the *AES* encryption format.
*   The *RSS 4000* recorder must be set to support encryption. For more information see the *RSS 4000 User Manual*.
*   Encryption must be selected in the *Conference Profile.*

Recording Link Encryption Flag Setting

Recording Links are treated as regular participants, however if the ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF *System Flag* is set to YES a non-encrypted *Recording Link* is to be allowed to connect to an encrypted conference.

Table 13-4 summarizes the connection possibilities for a *Recording Link* that is to be connected to a conference for each of the conference *profile* and *Entry Queue* encryption options.

Table 13-4   *Connections by Recording Link and Conference Encryption Settings*

Conference Profile Setting	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_ LINK_IN_ENCRYPT_CONF	
	YES	**NO**
Encrypt All	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected.
No Encryption	Connected non-encrypted.	Connected non-encrypted.
Encrypt when possible	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.

Recording Link Settings

The recording of encrypted conferences via an encrypted *Recording Link* is enabled in the *Conference Profile* by:

*   Selecting the *Encryption* option (**Encrypt All** or **Encrypt when Possible**) in the *Advanced* tab.

    For more details, see "*Media Encryption"* on page **4-27**.
*   Setting the Recording options in the *Recording* tab. For more details, see "*Enabling the Recording in the Conference Profile"* on page **13-5**.

Managing the Recording Process

When a conference is started and recording is enabled in its *Profile*, the system will automatically start the recording if the *Start Recording* parameter is set to *immediately*. If it is set to *Upon Request*, the system waits for the chairperson or *Collaboration Server* user's request. Once the recording is initiated for a conference, the MCU connects to the recording device (*RSS 2000/4000*) using the default *Recording Link*. The connection that is created between the conference and the recording device is represented as a special participant (Recording) whose name is the *Recording Link*. Once the recording has started, the recording process can be stopped and restarted from the Chairperson's endpoint (using DTMF codes) or from the *Polycom RealPresence Collaboration Server (RMX) 1800 Administrator's Guide Web Client*. After the recording process has finished, the recording can be identified in the *RSS 2000/4000* by its *Collaboration Server* conference name.

> A conference participant and the *Recording Link* cannot have identical names, otherwise the recording process will fail.

Recording Link Layout

When the video layout of the conference is set to *Auto Layout*, the recording of the conference will now include all the conference participants and not n-1 participants as in previous versions.

In the new *Auto Layout* algorithm, the *Recording Link* is counted as a "participant" and therefore it is excluded from the layout display used for the recording. The layout used for the other participants will behave as in the "standard" *Auto Layout* behavior.

The *Recording Link Layout* can be changed during an ongoing conference in the same manner as for any other conference participant. For more information see the "*Participant Level Monitoring*" on page **12-15**.

The default settings for *Auto Layout* for the conference and the *Recording Link* are summarized in the following table:

Table 14   *Recording Link Default Layout Settings (Auto Layout Mode)*

Participants	Conference Auto Layout Default Settings	Recording Link Auto Layout Settings
0	Not applicable	Not applicable
1		
2		
3		
4		
5		
6		
7		
8		
9		
10 or more		

The default settings for *Auto Layout* of the *Recording Link* cannot be changed, and the *Auto Layout* flags do not apply to the *Recording Link Auto Layout* default settings.

Using the Collaboration Server Web Client to Manage the Recording Process

To manage the recording process using the right-click menu:

>> Right-click the *Recording* participant in the conference and select from one of the following options:
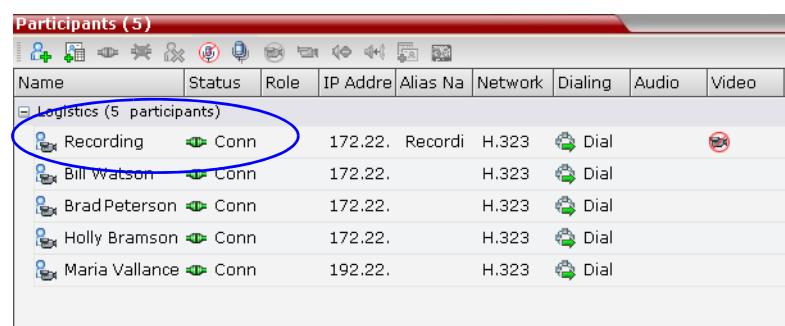
Table 13-1 Recording Participant Right-click Options

Name	Description
Start	Starts recording. When recording has started, this option toggles with the *Pause* option.
Pause	Pauses the recording of the conference without disconnecting. When the Recording is Paused, this option toggles with the *Start* option.
Resume	Resumes the recording of the conference. The Resume option toggles with the *Pause* option when it is used.
Stop	Stops the recording. **Note:** The Stop button is only enabled when the Recording is *Started* or *Paused*.
Suspend Video	The Suspend Video option prevents the incoming video of the recording link participant to be part of the conference layout. The Recording Link participant is set by default to Suspend Video. The Suspend Video option toggles with the Resume Video option.
Resume Video	The Resume Video option enables the incoming video of the recording link participant to be part of the conference layout. This feature may be used to play back previously recorded video or audio feeds in the conference layout. For more information, see the RSS 4000 User Guide.
Participant Properties	The Participant Properties option displays viewing only information for monitoring, e.g. communication capabilities and channels used to connect to the conference. Users will not be able to perform any functional requests from this window, i.e. disconnect, change layout and mute.

To manage the recording process using the Conference toolbar:

>> In the *Conferences* pane, click one of the following buttons in the Conference tool bar.
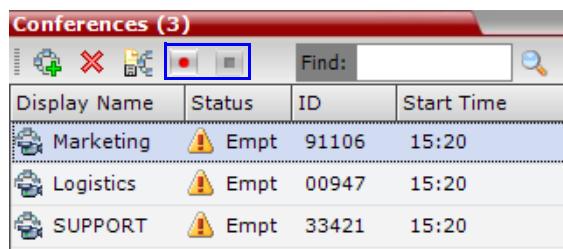
The recording buttons will only be displayed in the conference tool bar for a conference that is recording-enabled.

Table 13-2 Conferences List - Recording Tool bar buttons

Button	Description
	Start/Resume recording. This button toggles with the *Pause* button.

Table 13-2 *Conferences List - Recording Tool bar buttons (Continued)*

Button	Description
■	Stop recording.
❚❚	Pause recording. This button toggles with the *Start/Resume* button.

Using DTMF Codes to Manage the Recording Process

By entering the appropriate DTMF code on the endpoint, the chairperson can **Stop** the recording (*74), **Pause** it (*75), or **Start/Resume** the recording (*73). For more information on managing the recording process via DTMF codes, see the *RSS 2000 User's Guide*.

Recording between the *Collaboration Server* and the *Codian VCR* is enabled by adding an IP participant to the recorded conference that acts as a link between the conference and the recording device. This participant is identified as a recording link to the Codian *VCR* according to the product ID sent from the *VCR* during the connection phase, in the call setup parameters.

The video channel between the conference and the recording device is unidirectional where the video stream is sent from the conference to the recorder.

If the *Codian VCR* opens a video channel to the conference - this channel is excluded from the conference video mix.

To record a conference running on the Collaboration Server using Codian recorder:

>> In the conference, define or add a dial-out participant using the *Codian VCR* IP address as the address for dialing.

Once added to the conference, the *MCU* automatically connects the participant (the link to *Codian VCR*) and the recording is automatically started on the *Codian VCR*.

A connection can also be defined on the *Codian VCR*, dialing into the recorded conference using the *MCU* prefix and the *Conference ID* as for any other dial-in participant in the conference.

Monitoring the recording participant:

This connection is monitored as any other participant in the conference. The connection can also be monitored in the *Codian VCR* web client.

14

Users, Connections, and Notes

Users

Collaboration Server Web Client users are defined in the User's table and can connect to the MCU to perform various operations.

A maximum of 100 users can be defined per MCU.

User Types

The MCU supports the following user Authorization Levels:

— Administrator
— Operator
— Machine Account (Application-user)
— Administrator Read-only
— Chairperson
— Auditor

> Users with *Auditor* authorization level cannot connect to the *Collaboration Server* via the *RMX Manager* application and must use the *Collaboration Server* Web Client.

The authorization level determines a user's capabilities within the system.

Administrator

An administrator can define and delete other users, and perform all configuration and maintenance tasks.

Administrator Read-only

A user with Administrator permission with the same viewing and monitoring permissions of a regular Administrator. However, this user is limited to creating system backups and cannot perform any other configuration or conference related operation.

Operator

An Operator can manage Meeting Rooms, Profiles, Entry Queues, and SIP Factories, and can also view the *Collaboration Server* configurations, but cannot change them.

Administrator and Operator users can verify which users are defined in the system. Neither of them can view the user passwords, but an Administrator can change a password.

Chairperson

A Chairperson can only manage ongoing conferences and participants. The Chairperson does not have access to the *Collaboration Server* configurations and utilities.

Auditor

An **Auditor** can only view *Auditor Files* and audit the system.

Machine Account

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies. For more details, see "*Machine Account*" on page **14-6**.

Listing Users

The *Users* pane lists the currently defined users in the system and their authorization levels. The pane also enables the administrators to add and delete users.

The system is shipped with a default Administrator user called POLYCOM, whose password is POLYCOM. However, once you have defined other authorized Administrator users, it is recommended to remove the default user.

You can view the list of users that are currently defined in the system.

To view the users currently defined in the system:

1   In the *Collaboration Server Management* pane, click the **Users** () button.

The *Users* pane is displayed.

The list includes three columns: User Name, Authorization Level and Disabled.

The *User Name* is the login name used by the user to connect to the MCU.

The *Authorization* indicates the Authorization Level assigned to the User: *Administrator, Administrator Read-only, Operator, Chairperson* or *Auditor*.

Disabled indicates whether the user is disabled and cannot access the system unless enabled by the administrator. For more details, see "*Disabling a User*" on page **14-4**. *Locked* indicates whether the user has been locked out and cannot access the system unless enabled by the administrator.

Adding a New User

Administrators can add new users to the system.

> The User Name and Password must be in ASCII.

To add a new user to the system:

1   In the *Collaboration Server Management* pane, click the **Users** () button.

2   The *Users* pane is displayed.

3 Click the **New User** (![icon]) button or right-click anywhere in the pane and then click **New User**.

The *User Properties* dialog box opens.

4 In the *User Name* text box, enter the name of the new user. This is the login name used by the user when logging into the system.

5 In the *Password* text box, enter the new user's password. This will be the user's password when logging into the system.

6 In the *Authorization Level* list, select the user type: **Administrator, Administrator Read-Only, Operator, Chairperson** or **Auditor**.

7 **Optional. To associate a user with a machine**:

a In the *User Properties* dialog box, select the **Associate with a machine** check box.

b Enter the *FQDN* of the server that hosts the application who's application-user name is being added. Example: `cma1.polycom.com`

8 Click **OK**.
The *User Properties* dialog box closes and the new user is added to the system.

Deleting a User

To delete a user, you must have Administrator authorization. The last remaining Administrator in the *Users* list cannot be deleted.

1 In the *Collaboration Server Management* pane, click the **Users** (![icon]) button.

2 Select the user and click the **Delete** (![icon]) button or right-click the user and then click **Delete User**.

The system displays a confirmation message.

3 In the *confirmation* dialog box, select **Yes** to confirm or **No** to cancel the operation.

If you select **Yes**, the user name and icon are removed from the system.

Changing a User's Password

Users with Administrator authorization can change their own password and other users' passwords. Users with Operator authorization can change their own password.

To change a user's password:

1   In the *Collaboration Server Management* pane, click the **Users** (⊞) option.

2   Right-click the user and click **Change User Password**.

The *Change Password* dialog box opens.

3   Enter the *Old Password* (current), *New Password* and *Confirm the New Password*.

The Password must be in ASCII.

4   Click **OK**.

The user's password is changed.

Disabling a User

An administrator can disable an enabled user. An indication is displayed in the Users List when the User is disabled. An administrator can enable a disabled User.

To disable a user:

1   In the *Collaboration Server Management* pane, click the **Users** (⊞) button.

The Users pane is displayed.

2   In the *Users* pane, right-click the user to be disabled and select **Disable User** in the menu.
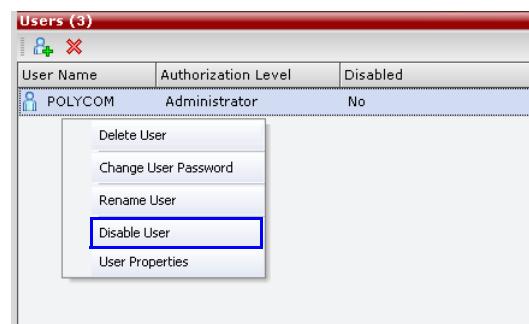
A confirmation box is displayed.
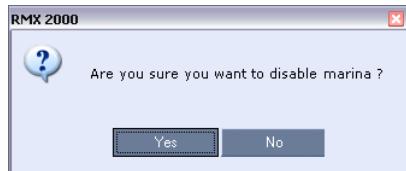
3   Click **YES**.
The User status in the *Users* list - *Disabled* column changes to **Yes**.

Enabling a User

An administrator can enable a User who was disabled manually by the administrator.

To enable a user:

1   In the *Collaboration Server Management* pane, click the **Users** ( ) button.

The *Users* pane is displayed.

2   Right-click the user to be enabled and select **Enable User**.

A confirmation box is displayed.

3   Click **YES**.
The User status in the *Users* list - *Disabled* column changes to **NO**.

Renaming a User

To rename a user:

1   In the *Collaboration Server Management* pane, click the **Users** ( ) button.

The Users pane is displayed.

2 Right-click the user to be renamed and select **Rename User**.

The *Rename User* dialog box is displayed.

3 Enter the user's new name in the *New User Name* field and click **OK**.

The user is renamed and is forced to change his/her password.

Machine Account

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies.

For enhanced security reasons it is necessary for the *Collaboration Server* to process user connection requests in the same manner, whether they be from regular users accessing the *Collaboration Server* via the *Collaboration Server Web Browser / RMX Manager* or from *application-users* representing applications such as *CMA* and *DMA*.

Regular users can connect from any workstation having a valid certificate while application-users representing applications can only connect from specific servers. This policy ensures that a regular user cannot impersonate an *application-user* to gain access to the *Collaboration Server* in order to initiate an attack that would result in a *Denial of Service* (*DoS*) to the impersonated application.

The connection process for an *application-user* connecting to the *Collaboration Server* is as follows:

1 The *application-user* sends a connection request, including its *TLS* certificate, to the *Collaboration Server*.

2 The *Collaboration Server* searches its records to find the *FQDN* that is associated with the *application-user's* name.

3 If the *FQDN* in the received certificate matches that associated with *application-user*, and the password is correct, the connection proceeds.

Guidelines

- *Application-users* are only supported when *TLS* security is enabled and *Request peer certificate* is selected. *TLS* security cannot be disabled until all *application-user* accounts have been deleted from the system.

- For *Secure Communications*, an administrator must set up on the *Collaboration Server* system a machine account for the *CMA/DMA/XMA* system with which it interacts. This machine account must include a fully-qualified domain name (*FQDN*) for the *CMA/DMA/XMA* system.

- *Application-user* names are the same as regular user names.
  Example: the *CMA* application could have an *application-user* name of `CMA1`.

- The *FQDN* can be used to associate all user types: *Administrator*, *Operator* with the *FQDN* of a server.

- Multiple *application-users* can be configured the same *FQDN* name if multiple applications are hosted on the same server

- If the system is downgraded the *application-user's FQDN* information is not deleted from the *Collaboration Server*'s user records.

- A *System Flag,* **PASS_EXP_DAYS_MACHINE,** enables the administrator to change the password expiration period of *application-user's* independently of regular users. The default flag value is 365 days.

- The server hosting an *application-user* whose password is about to expire will receive a login response stating the number of days until the *application-user's* password expires. This is determined by the value of the **PASSWORD_EXPIRATION_WARNING_DAYS** *System Flag*. The earliest warning can be displayed 14 days before the password is due to expire and the latest warning can be displayed 7 days before passwords are due to expire. An *Active Alarm* is created stating the number of days before the password is due to expire.

- The **MIN_PWD_CHANGE_FREQUENCY_IN_DAYS** *System Flag* does not effect *application-user* accounts. Applications typically manage their own password change frequency.

- If an *application-user* identifies itself with an incorrect *FQDN*, its account will not be locked, however the event is written to the *Auditor Event File*.

- If an *application-user* identifies itself with a correct *FQDN* and an incorrect password, its account will be locked and the event written to the *Auditor Event File*.

- An *application-user* cannot be the last administrator in the system. The last administrator must be regular user.

- User names are not case sensitive.

Monitoring

- An *application-user* and its connection is represented by a specific icon.

Active Directory

- When working with *Active Directory*, *CMA, DMA,* and *XMA* cannot be registered within *Active Directory* as regular users. *CMA* and *DMA application-users* must be manually.

- The only restriction is that TLS mode is enabled together with client certificate validation.

- If the above configuration are set off it will not be possible to add machine accounts.

• When setting the TLS mode off the system should check the existence of a machine account and block this operation until all machine accounts are removed.

Connections

The *Collaboration Server* enables you to list all connections that are currently logged into the MCU, e.g. users, servers or API users. The MCU issues an ID number for each login. The ID numbers are reset whenever the MCU is reset.

A maximum of 50 users can be concurrently logged in to the MCU.

Viewing the Connections List

To list the users who are currently connected to the MCU:

1   In the *Collaboration Server Management* pane, click the **Connections** ( ) button.

A list of connected users is displayed in the *Connections* pane.

The information includes:

— The user's login name.
— The user's authorization level (Chairperson, Operator, Administrator or Auditor).
— The time the user logged in.
— The name/identification of the computer used for the user's connection.

Notes

Notes are the electronic equivalent of paper sticky notes. You can use notes to write down questions, important phone numbers, names of contact persons, ideas, reminders, and anything you would write on note paper. *Notes* can be left open on the screen while you work.

Notes can be read by all system Users concurrently connected to the MCU. Notes that are added to the *Notes* list are updated on all workstations by closing and re-opening the *Notes* window. Notes can be written in any Unicode language.

Using Notes

To create a note:

1 On the *Collaboration Server* menu, click **Administration > Notes**.

The *Notes* window opens.
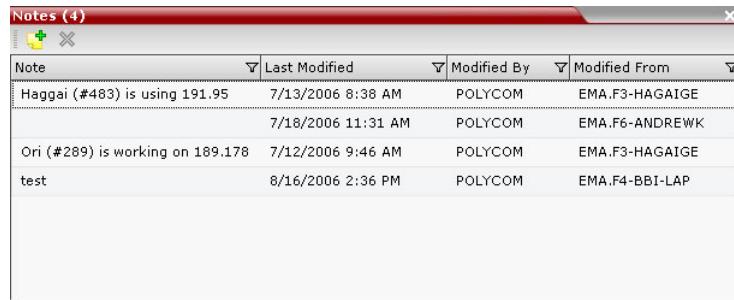
2 In the *Notes* toolbar, click the **New Note** ( ) button, or right-click anywhere inside the *Notes* window and select **New Note**.

3 In the *Note* dialog box, type the required text and click **OK**.

The new note is saved and closed. The *Notes* list is updated, listing the new note and its properties:

— **Note** – The beginning of the note's text.

— **Last Modified** – The date of creation or last modification.

— **Modified By** – The *Login Name* of the user who last modified the note.

— **Modified From** – The *Client Application* and *Workstation* from which the note was created or modified.
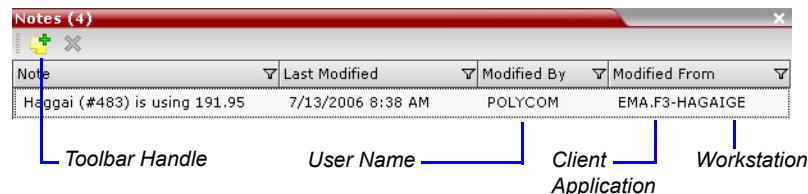
To open or edit a note:

4 Double-click the entry to edit, or right-click the entry and select **Note Properties**.

The note opens for viewing or editing.

To delete a note:

1   In the *Notes* list, select the entry for the note to delete and click the **Delete Note** button
     ( ), or right-click the entry and select **Delete Note**.

     A *delete confirmation* dialog box is displayed.

2   Click **OK** to delete the note, or click **Cancel** to keep the note.

15

IVR Services

Interactive Voice Response (IVR) is an application that allows participants to communicate with the conferencing system via their endpoint's input device (such as a remote control). The IVR Service includes a set of voice prompts and a video slide used to automate the participants connection to a conference or Entry Queue. It allows customization of menu driven scripts and voice prompts to meet different needs and languages.

The IVR module includes two types of services:

- Conference IVR Service that is used with conferences
- Entry Queue IVR Service that is used with Entry Queues

The system is shipped with two default Conference IVR Services (one for the conferences and the other for gateway calls) and one default Entry Queue IVR Service. The default services include voice messages and video slides in English.

To customize the IVR messages and video slide perform the following operations:

- Record the required voice messages and create a new video slide. For more information, see *"Creating a Welcome Video Slide"* on page **15-30**.
- Optional. Add the language to the list of languages supported by the system.
- Upload the voice messages to the MCU (This can be done as part of the language definition or during the IVR Service definition).
- Create the Conference IVR Service and upload the video slide, and if required any additional voice messages.
- Optional. Create the Entry Queue IVR Service and upload the required video slide and voice messages.

IVR Services List

You can view the currently defined Conference IVR and Entry Queue IVR Services in the *IVR Services* list pane.

To view the IVR Services list:

1 In the *Collaboration Server Management* pane, expand the *Rarely Used* list.

2 Click the **IVR Services** (▦) entry.

The list pane displays the *Conference IVR Services* list and the total number of IVR services currently defined in the system.

IVR Toolbar   IVR Services List Pane

Access to IVR Services
list and customization
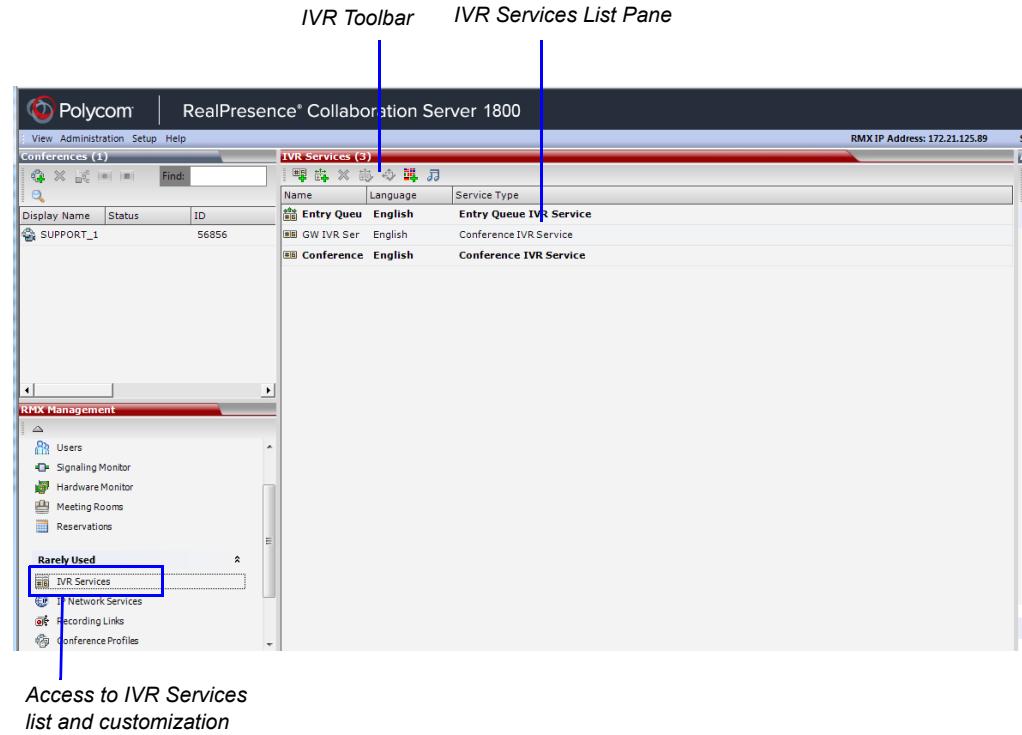
IVR Services Toolbar

The IVR Services toolbar provides quick access to the IVR Service definitions as follows:

Table 15-1   IVR Toolbar buttons

Button	Button Name	Descriptions
	New Conference IVR Service	To create a new Conference IVR Service.
	New Entry Queue IVR Service	To create a new Entry Queue IVR Service.
	Delete Service	Deletes the selected IVR service(s).
	Set Default Conference IVR Service	Sets the selected Conference IVR Service as default. When creating a new conference Profile the default IVR Service is automatically selected for the Profile (but can be modified).
	Set Default Entry Queue Service	Sets the selected Entry Queue IVR Service as default. When creating a new Entry Queue the default Entry Queue IVR Service is automatically selected.

Table 15-1 *IVR Toolbar buttons*

Button	Button Name	Descriptions
	Add Supported Languages	Adds languages to the IVR module, enabling you to download voice prompts and messages for various languages.
	Replace/Change Music File	To replace the currently loaded music file that is used to play background music, the MCU is shipped with a default music file.

Adding Languages

You can define different sets of audio prompts in different languages, allowing the participants to hear the messages in their preferred language.

The *Collaboration Server* is shipped with a default language (English) and all the prompts and messages required for the default IVR Services, conference and Entry Queues shipped with the system.

You can add languages to the list of languages for which different messages are downloaded to the MCU and IVR Services are created. This step is required before the creation of additional IVR messages using languages that are different from English, or if you want to download additional voice files to existing files in one operation and not during the IVR service definition.

To add a language:

1   In the *Collaboration Server Management* pane, expand the **Rarely Used** list.

2   Click the **IVR Services** ( ) entry.

3   In the *Conference IVR Services* list, click the **Add Supported Languages** ( ) button. The *Supported Languages* dialog box opens.
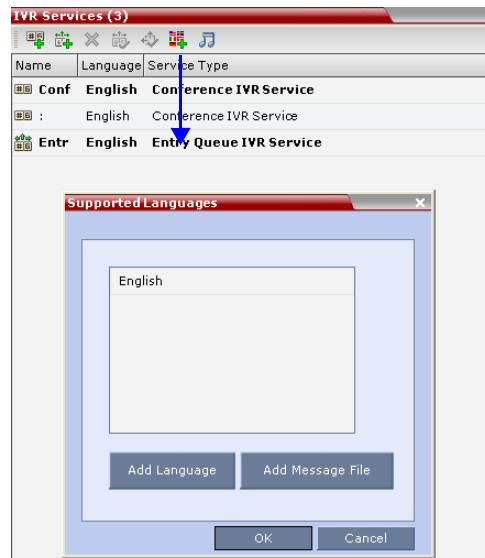
4   Click the **Add Language** button.

The *New Language* dialog box opens.
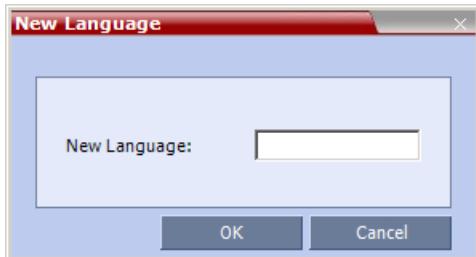
5 In the *New Language* box, enter the name of the new language. The language name can be typed in Unicode and cannot start with a digit. Maximum field length is 31 characters.

6 Click **OK**.
The new language is added to the list of *Supported Languages*.

Uploading a Message File to the Collaboration Server

You can upload audio files for the new language or additional files for an existing language now, or you can do it during the definition of the IVR Service. In the latter case, you can skip the next steps.

> • Voice messages should not exceed 3 minutes.
> • It is not recommended to upload more than 1000 audio files to the MCU memory.

To upload messages to the MCU:

1 To upload the files to the MCU, in the *Supported Languages* dialog box, click the **Add Message File** button.

2 The *Add Message File* dialog box opens.

Audio files are uploaded to the MCU one-by-one.

3 In the *IVR Message Language* list, select the language for which the audio file will be uploaded to the MCU.

4 In the *IVR Message Category* list, select the category for which the audio file is uploaded.

5 In the *Message Type* list, select the message type for which the uploaded message is to be played. You can upload several audio files for each Message Type. Each file is downloaded separately.

Table 15-2 lists the Message Types for each category:

Table 15-2 IVR Message Types by Message Category

Message Category	Message Type	Message
Conference Password	Request Conference Password	Requests the participant to enter the conference password.
	Request Conference Password Retry	A participant who enters an incorrect password is requested to enter it again.
	Request Digit	Requests the participant to enter any digit in order to connect to the conference. Used for dial-out participants to avoid answering machines in the conference.
Welcome Message	Welcome Message	The first message played when the participant connects to the conference or Entry Queue.
Conference Chairperson	Request Chairperson Identifier	Requests the participants to enter the chairperson identifier key.
	Request Chairperson Password	Requests the participant to enter the chairperson password.
	Request Chairperson Password Retry	When the participant enters an incorrect chairperson password, requests the participant to enter it again.
General		Messages played for system related event notifications, for example, notification that the conference is locked. Upload the files for the voice messages that are played when an event occurs during the conference. For more information, see "*Conference IVR Service Properties - General Voice Messages"* on page **15-11**.
Billing Code		Requests the chairperson to enter the conference Billing Code.
Roll Call		Not applicable.
Conference ID		Requests the participant to enter the required Conference ID to be routed to the destination conference.

6 Click **Upload File** to upload the appropriate audio file to the MCU.
The *Install File* dialog box opens.

7 Enter the file name or click the **Browse** button to select the audio file to upload.
The *Select Source File* dialog box opens.

8   Select the appropriate *.wav audio file, and then click the **Open** button.
     The name of the selected file is displayed in the *Install* field in the *Install File* dialog box.

9   Optional. You can play a .wav file by selecting the *Play* button ( ).

10   Click **Yes** to upload the file to the MCU.
     The system returns to the *Add Message File* dialog box.

11   Repeat step 6 to 10 for each additional audio file to be uploaded to the MCU.

12   Once all the audio files are uploaded to the MCU, close the *Add Message File* dialog box
     and return to the *Add Language* dialog box.

13   Click **OK**.

Defining a New Conference IVR Service

The *Collaboration Server* is shipped with two default Conference IVR Services and all its
audio messages and video slide. You can define new Conference IVR Services or modify the
default Conference IVR Service.

> Up to 40 IVR Services (Conference IVR Services and Entry Queue IVR Services) can be defined for
> a single *Collaboration Server* unit.

Defining a New Conference IVR Service

To define a new Conference IVR Service:

1   On the *IVR Services* toolbar, click the **New Conference IVR Service** ( ) button.
     The *New Conference IVR Service - Global* dialog box opens.
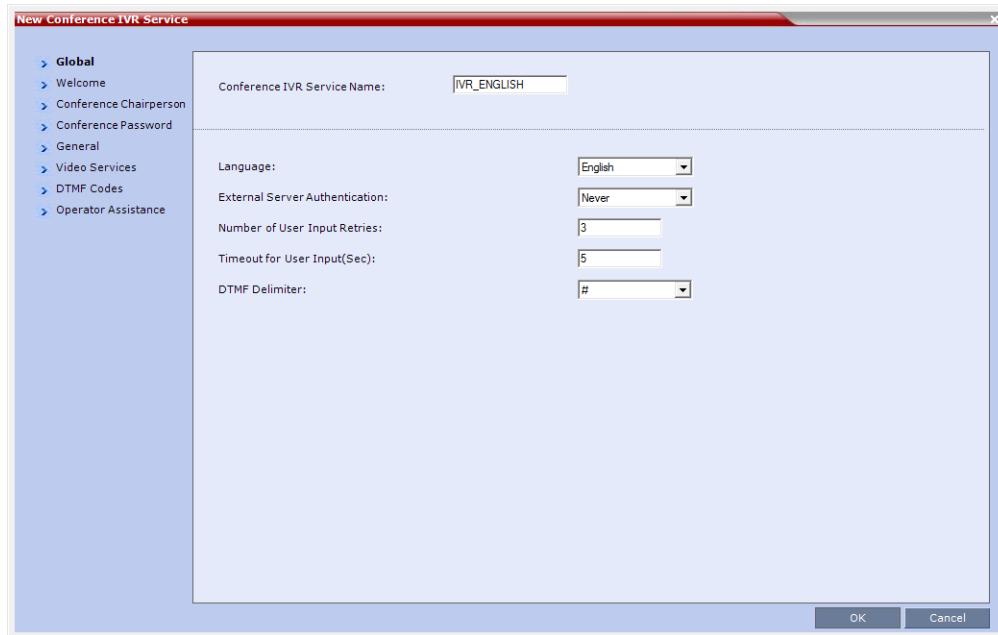
2 Define the following parameters:

Table 15-3 Conference IVR Service Properties - Global Parameters

Field/Option	Description
Conference IVR Service Name	Enter the name of the Conference IVR Service. The maximum field length is 20 characters and may be typed in Unicode.
Language For IVR	Select the language of the audio messages and prompts from the list of languages defined in the *Supported languages*. The default language is English. For more information, see "*Adding Languages*" on page **15-3**.
External Server Authentication	This option is not supported with RMX 1800.
Number of User Input Retries	Enter the number of times the participant will be able to respond to each menu prompt before being disconnected from the conference. Range is between 1-4, and the default is 3.
Timeout for User Input (Sec)	Enter the duration in seconds that the system will wait for the participant's input before prompting for another input. Range is between 1-10, and the default value is 5 seconds.
DTMF Delimiter	Enter the key that indicates the last input key. Possible values are the pound (#) and star (*) keys. The default is #.

3 Click the **Welcome** tab.
The *New Conference IVR Service - Welcome* dialog box opens.
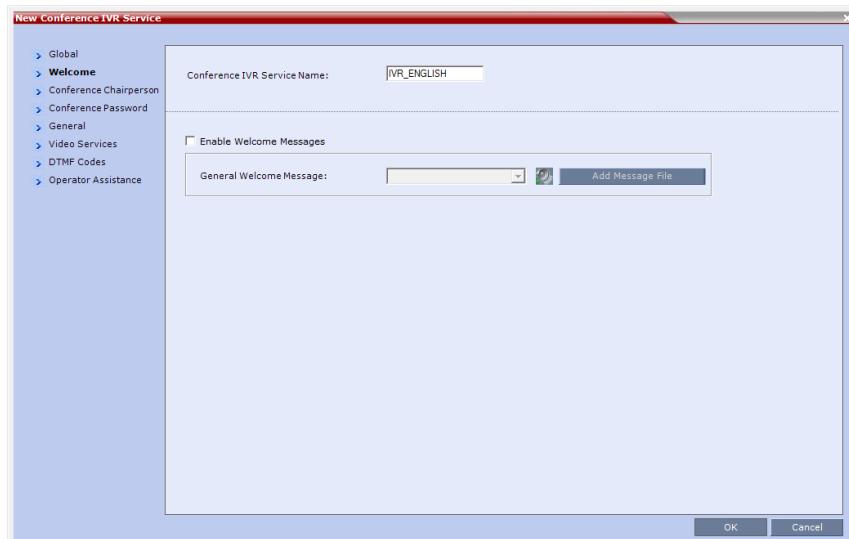
4 Select the **Enable Welcome Messages** check box to define the system behavior when the participant enters the Conference IVR queue. When participants access a conference through an Entry Queue, they hear messages included in both the Entry Queue Service and Conference IVR Service. To avoid playing the Welcome Message twice, disable the Welcome Message in the Conference IVR Service.

5 Select the **General Welcome Message,** to be played when the participant enters the conference IVR queue.

6 To upload an audio file for an IVR message, click **Add Message File**.
The *Install File* dialog box opens.

The *Collaboration Server* unit is bundled with default audio IVR message files. To upload a customized audio file, see *"Creating Audio Prompts and Video Slides"* on page **15-27**.

---

a Click the **Browse** button to select the audio file (*.wav) to upload.
The *Select Source File* dialog box opens.

b Select the appropriate *.wav audio file and then click the **Open** button.

c Optional. You can play a .wav file by selecting the *Play* button ( ).

d In the *Install File* dialog box, click **Yes** to upload the file to the MCU memory.
The *Done* dialog box opens.

e Once the upload is complete, click **OK** and return to the *IVR* dialog box. The new audio file can now be selected from the list of audio messages.

7 Click the **Conference Chairperson** tab.
The *New Conference IVR Service - Conference Chairperson* dialog box opens.
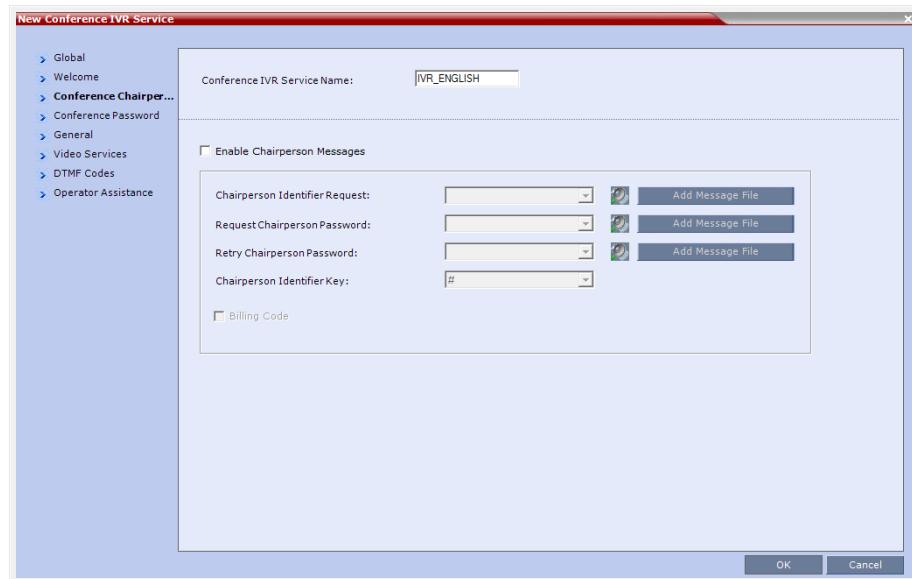
8 Select the **Enable Chairperson Messages** check box to enable the chairperson functionality. If this feature is disabled, participants are not able to connect as the chairperson.

> When both Conference Password and Chairperson Password options are enabled and defined, the system first plays the prompt "Enter conference password". However, if the participant enters the chairperson password, the participant becomes the chairperson.
> To play the prompt requesting the Chairperson password, "For conference chairperson services...", **do not select** the *Enable Password Messages* option.

9 Select the various voice messages and options for the chairperson connection.

> If the files were not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the *Collaboration Server*.

Table 15-4 *New Conference IVR Service Properties - Conference Chairperson Options and Messages*

Field/Option	Description
Chairperson Identifier Request	Select the audio file that requests the participants to enter the key that identifies them as the conference chairperson.
Request Chairperson Password	Select the audio file that prompts the participant for the chairperson password.
Retry Chairperson Password	Select the audio file that prompts participants to re-enter the chairperson password if they enter it incorrectly.
Chairperson Identifier Key	Enter the key to be used for identifying the participant as a chairperson. Possible keys are: pound key (#) or star (*).
Billing Code	The prompt requesting the chairperson billing code selected in the General tab.

10 Click the **Conference Password** tab.

The *New Conference IVR Service - Conference Password* dialog box opens.
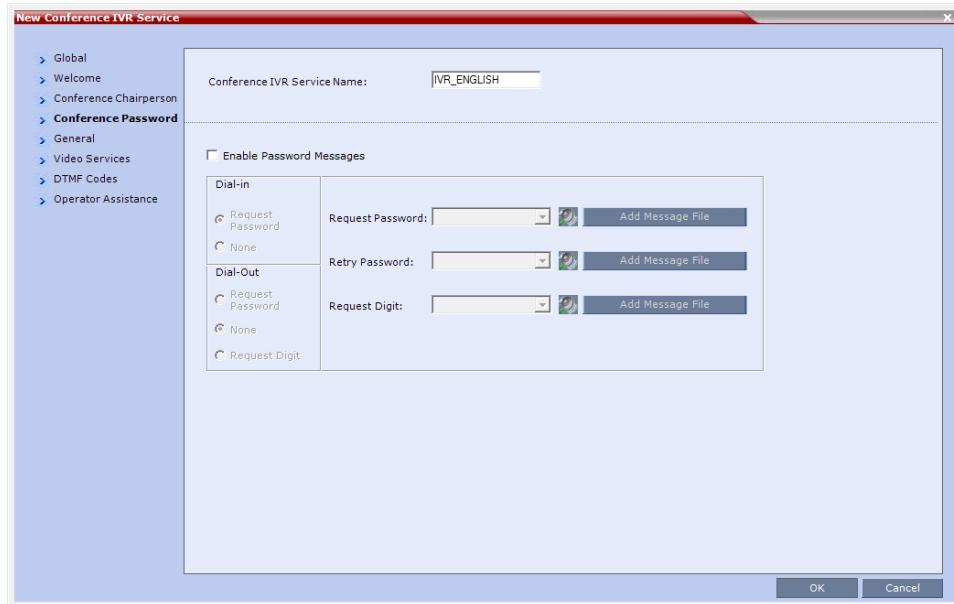
11 Select the **Enable Password Messages** check box to request the conference password before moving the participant from the conference IVR queue to the conference.

> When both Conference Password and Chairperson Password are enabled and defined, the system first plays the prompt "Enter conference password". However, if the participant enters the chairperson password, the participant becomes the chairperson.
> To play the prompt requesting the Chairperson password, "For conference chairperson services...", **do not select** the *Enable Password Messages* option.

12 Select the MCU behavior for password request for *Dial-in* and *Dial-out* participant connections.

Select the required system behavior as follows:

— **Request password** - The system requests the participant to enter the conference password.

— **None** - The participant is moved to the conference without any password request.

— **Request Digit** - The system requests the participant to enter any key. This option is used mainly for dial-out participants and to prevent an answering machine from entering the conference.

13 Select the various audio messages that will be played in each case.

Table 15-5 *New Conference IVR Service Properties - Conference Password Parameters*

Option	Description
Request Password	Select the audio file that prompts the participant for the conference password.
Retry Password	Select the audio file that requests the participant to enter the conference password again when failing to enter the correct password.

Table 15-5 *New Conference IVR Service Properties - Conference Password Parameters*

Option	Description
Request Digit	Select the audio file that prompts the participant to press any key when the *Request Digit* option is selected.

14 Click the **General** tab.

The *New Conference IVR Service - General* dialog box opens.
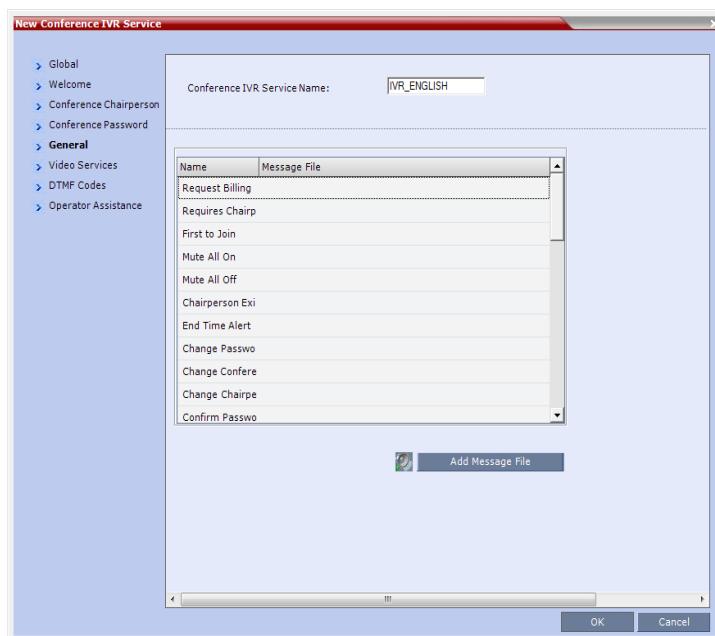
The *General* dialog box lists messages that are played during the conference. These messages are played when participants or the conference chairperson perform various operations or when a change occurs.

15 To assign the appropriate audio file to the message type, click the appropriate table entry, in the *Message File* column. A drop-down list is enabled.

16 From the list, select the audio file to be assigned to the event/indication.

17 Repeat steps 15 and 16 to select the audio files for the required messages.

The following types of messages and prompts can be enabled:

Table 15-6 *Conference IVR Service Properties - General Voice Messages*

Message Type	Description
Blip on Cascade Link	Indicates that the link to the cascaded conference connected successfully.
Chairperson Exit	Informs all the conference participants that the chairperson has left the conference, causing the conference to automatically terminate after a short interval. **Note:** This message is played only when the *Requires Chairperson* option is selected in the *Conference Profile - IVR* dialog box.

Table 15-6 Conference IVR Service Properties - General Voice Messages (Continued)

Message Type	Description
Chairperson Help Menu	A voice menu is played upon a request from the chairperson, listing the operations and their respective DTMF codes that can be performed by the chairperson. The playback can be stopped any time. **Note:** If you modify the default DTMF codes used to perform various operations, the default voice files for the help menus must be replaced.
Change Chairperson Password	Requests the participant to enter a new chairperson password when the participant is attempting to modify the chairperson password.
Change Conference Password	Requests the participant to enter a new conference password when the participant is attempting to modify the conference password.
Change Password Failure	A message played when the participant enters an invalid password, for example when a password is already in use.
Change Passwords Menu	This voice menu is played when the participants requests to change the conference password. This message details the steps required to complete the procedure.
Conference is Locked	This message is played to participants attempting to join a Secured conference.
Conference is Secured	This message is played when the conference status changes to Secure as initiated by the conference chairperson or participant (using DTMF code *71).
Conference is unsecured	This message is played when the conference status changes to Unsecured as initiated by the conference chairperson or participant (using DTMF code #71).
Confirm Password Change	Requests the participant to re-enter the new password.
Enter Destination ID	Prompts the calling participant for the destination number. Default message prompts the participant for the conference ID (same message as in the Entry Queue IVR Service).
First to Join	Informs the participant that he or she is the first person to join the conference.
Incorrect Destination ID	If the participant entered an incorrect conference ID (in gateway calls it is the destination number), requests the participant to enter the number again.
Maximum Number of Participants Exceeded	Indicates the participant cannot join the destination conference as the maximum allowed number of participants will be exceeded.
Mute All Off	This message is played to the conference to inform all participants that they are unmuted (when *Mute All* is cancelled).

Table 15-6 *Conference IVR Service Properties - General Voice Messages (Continued)*

Message Type	Description
Mute All On	Informs all participants that they are muted, with the exception of the conference chairperson. **Note:** This message is played only when the *Mute All Except Me* option is activated.
No Video Resources Audio Only.	Informs the participant of the lack of Video Resources in the *Collaboration Server* and that he/she is being connected as Audio Only.
Participant Help Menu	A voice menu that is played upon request from a participant, listing the operations and their DTMF codes that can be performed by any participant.
Password Changed Successfully	A message is played when the password was successfully changed.
Recording Failed	This message is played when the conference recording initiated by the chairperson or the participant (depending on the configuration) fails to start.
Recording in Progress	This message is played to participant joining a conference that is being recorded indicating the recording status of the conference.
Request Billing Code	Requests the participant to enter a code for billing purposes.
Requires Chairperson	The message is played when the conference is on hold and the chairperson joins the conference. For this message to be played the *Conference Requires Chairperson* option must be selected in the *Conference Profile - IVR* dialog box.
Self Mute	A confirmation message that is played when participants request to mute their line.
Self Unmute	A confirmation message that is played when participants request to unmute their line.

18 Click the **Video Services** tab.

The *New Conference IVR Service - Video Services* dialog box opens.
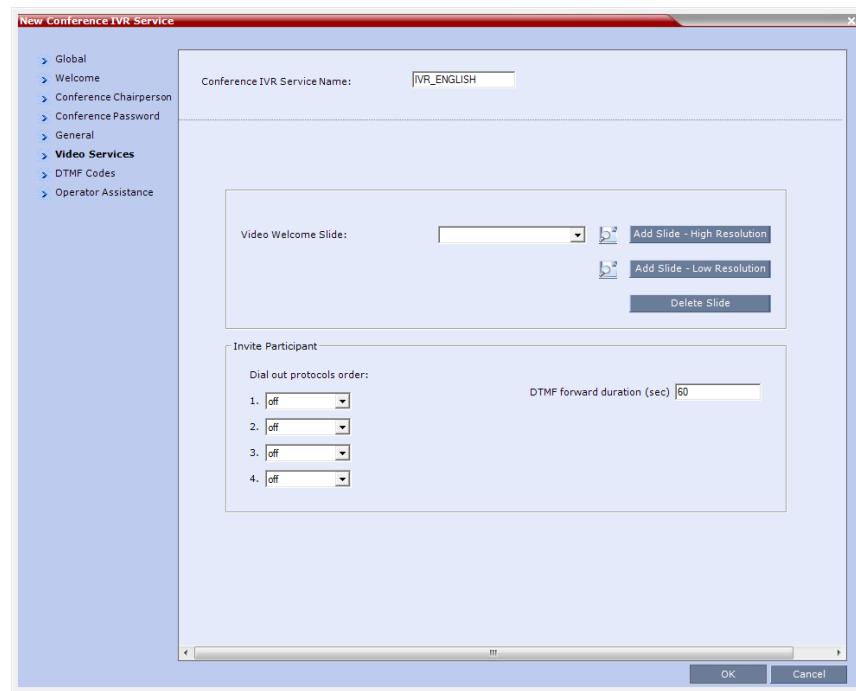
In addition to the low and high resolution slides included in the default slide set, customized low and high resolution slides are supported.

The following guidelines apply:

— Two customized slides can be loaded per *IVR Service*:

- • A low resolution slide, to be used with low resolution endpoints.
- • A high resolution slide, to be used with high resolution endpoints.

Table 15-7 summarizes the recommended input slide formats and the resulting slides that are generated:

Table 15-7 IVR Slide - Input / Output Formats

Slide Resolution	Format	
	Input Slides	**Generated Slides**
High	HD1080p (16:9) or HD720p (16:9)	HD1080p HD720p
Low	4CIF (4:3) or CIF (4:3)	4SIF SIF CIF

— The source images for the high resolution slides must be in *.bmp* or *.jpg* format.

— If the uploaded slides are not of the exact *SD* or *HD* resolution, an error message is displayed and the slides are automatically cropped or enlarged to the right size.

— If a slide that is selected in an *IVR Service* is deleted, a warning is displayed listing the *IVR Services* in which it is selected. If deleted, it will be replaced with a default *Collaboration Server* slide.

— The generated slides are not deleted if the system is downgraded to a lower software version.

— The first custom source file uploaded, whatever its format, is used to generate both high and low resolution custom slides. High resolution source files uploaded after the first upload will be used to generate and replace high resolution custom slides. Likewise, low resolution source files uploaded after the first upload will be used to generate and replace low resolution custom slides.

— If there are two custom source files in the folder, one high resolution, one low resolution, and a new high resolution custom source file is uploaded, new high resolution custom slides are created. The existing low resolution custom slides are not deleted.

— If there are two custom source files in the folder, one high resolution, one low resolution, and a new low resolution custom source file is uploaded, new low resolution custom slides are created. The existing high resolution custom slides are not deleted.

19 Define the following parameters:

Table 15-8 New Conference IVR Service Properties - Video Services Parameters

Video Services	Description
Video Welcome Slide	Select the *Low Resolution* and *High Resolution* video slides to be displayed when participants connect to the conference.
	To view any slide, click the **Preview Slide** () button.
	Notes:
	• When using one of the default Polycom slides, the slide will be displayed in the resolution defined in the profile, i.e. CIF, SD, HD 720p or HD 1080p. When defining a gateway IVR Service, the recommended default slide is: Default_GW_Welcome_Slide.
	• Customized H.261 slides are not supported.
Invite Participant	Not applicable.
	Note: The Invite Participant feature is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.

20 If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the:

— **Add Slide - Low Resolution** button to upload a *Low Resolution Slide*.

— **Add Slide - High Resolution** button to upload a *High Resolution Slide*.

The *Install File* dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step **6** on page **15-8**.

> • The video slide must be in a .jpg or .bmp file format. For more information, see "*Creating a Welcome Video Slide"* on page **15-30**.
> • Customized H.261 slides are not supported.

21 Click the **DTMF Codes** tab.

The *New Conference IVR Service - DTMF Codes* dialog box opens.
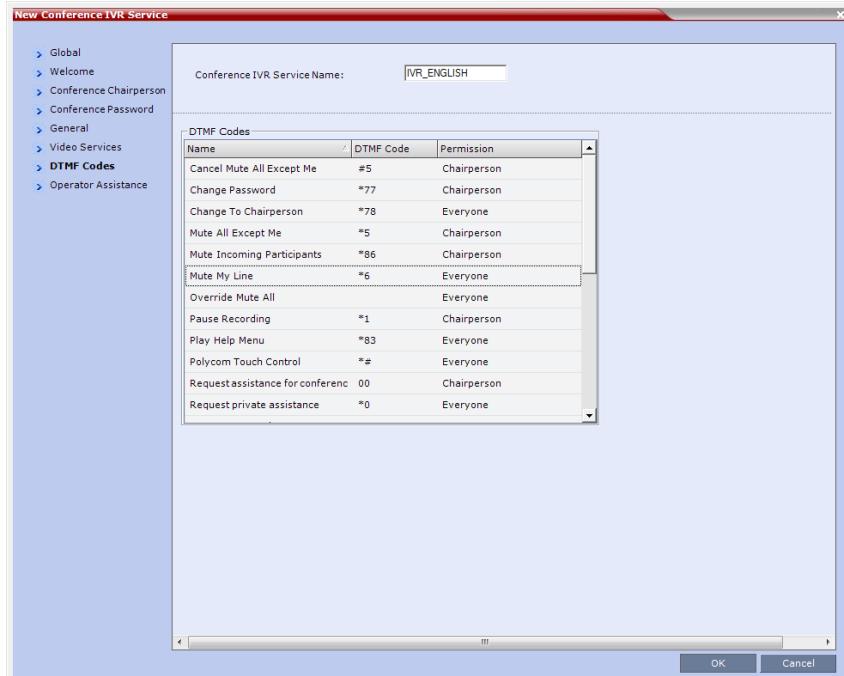
• This dialog box lists the default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson.

Table 15-9 New Conference IVR Service Properties - DTMF Codes

Operation	DTMF String	Permission
Mute My Line	*6	Everyone
Unmute My Line	#6	Everyone
Mute All Except Me	*5	Chairperson
Cancel Mute All Except Me	#5	Chairperson
Change Password	*77	Chairperson
Mute Incoming Participants	*86	Chairperson
Unmute Incoming Participants	#86	Chairperson
Play Help Menu	*83	Everyone
Terminate Conference	*87	Chairperson

Table 15-9 *New Conference IVR Service Properties - DTMF Codes*

Operation	DTMF String	Permission
Change To Chairperson	*78	Everyone
Override Mute All	Configurable	Everyone
Start Recording	*3	Chairperson
Stop Recording	*2	Chairperson
Pause Recording	*1	Chairperson
Secure Conference	*71	Chairperson
Unsecured Conference	#71	Chairperson
Request individual assistance	*0	Everyone
Request assistance for conference	00	Chairperson
Request to Speak	99	Everyone

22 To modify the DTMF code or permission:

a In the *DTMF Code* column, in the appropriate entry enter the new code.

b In the *Permission* column, select from the list who can use this feature (Everyone or just the Chairperson).

By default, the Secure, Unsecure Conference and Show Number of Participants options are enabled in the Conference IVR Service. These options can be disabled by removing their codes from the Conference IVR Service.

• To disable the Secure Conference options, in the *DTMF Code* column, clear the DTMF codes of both Secured Conference **(*71)** and Unsecured Conference **(#71)** from the table.

23 Click the **Operator Assistance** tab.

The *Operator Assistance* dialog box opens.
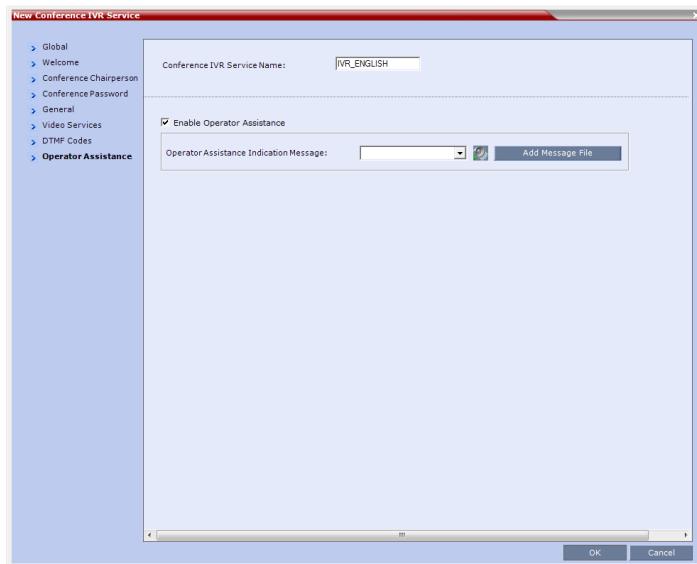
24 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process to the conference or during the conference.

25 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for the operator's assistance.

> If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the *Collaboration Server*.

26 Click **OK** to complete the IVR Service definition.

The new Conference IVR Service is added to the *IVR Services* list.

Change to Chairperson

Regular participants can request to become the conference chairperson using the appropriate DTMF code (default: *78), which enabled them to perform operations designated for chairpersons only.

The Change to Chairperson via the DTMF code (default: *78) is executed only if the following settings were configured for the MCU and the conference:

* In the *Conference IVR Service - Conference Chairperson* dialog box, select the **Enable Chairperson Messages** check box, and select the appropriate voice messages.

    For more information, see *Polycom RealPresence Collaboration Server (RMX) 1800 Administrator's Guide*, *"New Conference IVR Service Properties - Conference Chairperson Options and Messages"* on page **15-9**.

* When starting a new conference or defining a new Meeting Room, define the *Chairperson Password* in the conference General dialog box.

    For more information, see *"Creating a New Meeting Room"* on page **6-4**.

Entry Queue IVR Service

An Entry Queue (EQ) is a routing lobby for conferences. Participants are routed to the appropriate conference according to the conference ID they enter.

An Entry Queue IVR Service must be assigned to the Entry Queue to enable the voice prompts and video slide guiding the participants through the connection process.

An Entry Queue IVR Service is a subset of an IVR Service. You can create different Entry Queue Services for different languages and personalized voice messages.

The *Collaboration Server* is shipped with a default Entry Queue IVR Service and all its audio messages and video slide. You can define new Entry Queue IVR Services or modify the default Entry Queue IVR Service.

Defining a New Entry Queue IVR Service

To set up a new Entry Queue IVR Service:

1 In the *RMX Management* pane, click **IVR Services** (▦).

2 In the *IVR Services* list, click the **New Entry Queue IVR Service** (▦) button.

The *New Entry Queue IVR Service - Global* dialog box opens.
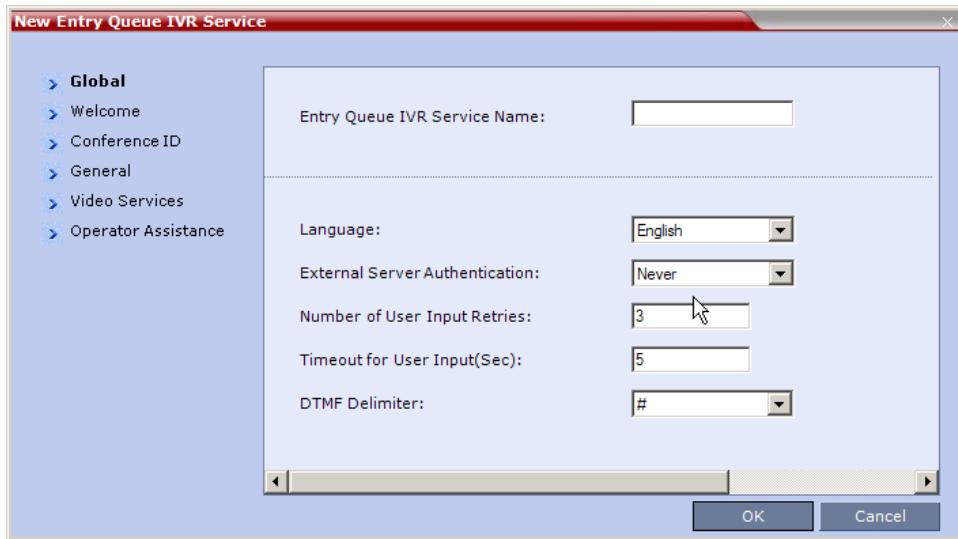
3 Fill in the following parameters:

Table 15-10 Entry Queue IVR Service Properties - Global Parameters

Option	Description
Entry Queue Service Name	(Mandatory) Enter the name of the Entry Queue Service. The name can be typed in Unicode. Maximum field length is 80 ASCII characters.
Language	Select the language in which the Audio Messages and prompts will be heard. The languages are defined in the *Supported Languages* function.

Table 15-10 Entry Queue IVR Service Properties - Global Parameters (Continued)

Option	Description
External Server Authentication	This option is used for Ad Hoc conferencing, to verify the participant's permission to initiate a new conference. For a detailed description see *Appendix D:* "*Ad Hoc Conferencing"* on page **D-1**. Select one of the following options: • **None** to start a new conference without verifying with an external database the user right to start it. • **Conference ID** to verify the user's right to start a new conference with an external database application using the conference ID.
Number of User Input Retries	Enter the number of times the participant is able to respond to each menu prompt before the participant is disconnected from the MCU.
Timeout for User Input (Sec.)	Enter the duration in seconds that the system waits for input from the participant before it is considered as an input error.
DTMF Delimiter	The interaction between the caller and the system is done via touch-tone signals (DTMF codes). Enter the key that will be used to indicate a DTMF command sent by the participant or the conference chairperson. Possible keys are the pound key (#) or star (*).

4 Click the **Welcome** tab.
The *New Entry Queue IVR Service - Welcome* dialog box opens.
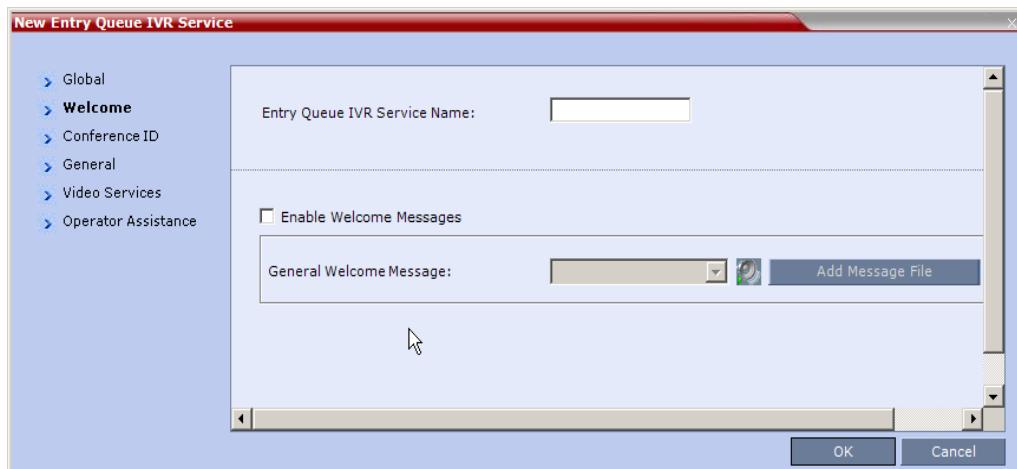
> If the files were not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the *Collaboration Server*.

5 Define the appropriate parameters. *T*his dialog box contains options that are identical to those in the *Conference IVR Service - Welcome Message* dialog box. For more information about these parameters, see Table 15-4 on page **15-9**.

6 Click the **Conference ID** tab.

The *New Entry Queue IVR Service - Conference ID* dialog box opens.
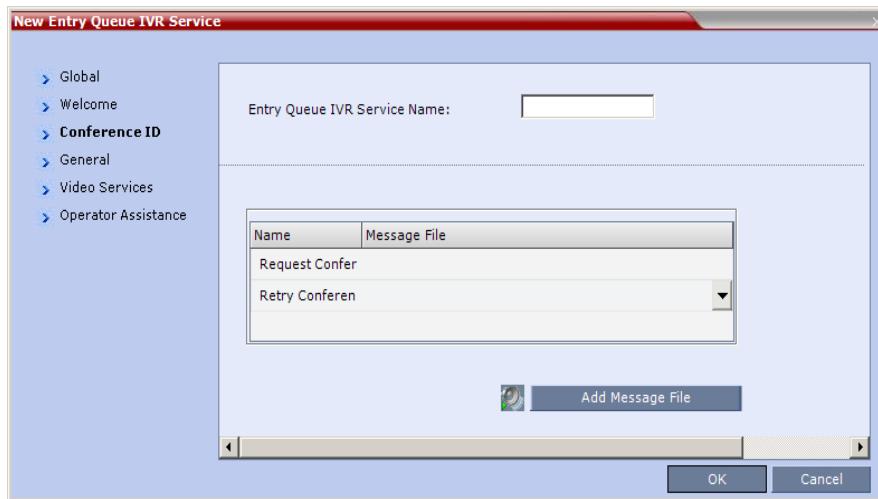
7 Select the voice messages:

Table 15-11 Entry Queue IVR Service Properties - Conference ID

Field/Option	Description
Request Conference ID	Prompts the participant for the conference ID.
Retry Conference ID	When the participant entered an incorrect conference ID, requests the participant to enter the ID again.

8 Assign an audio file to each message type, as follows:

— In the *Message File* column, click the table entry, and then select the appropriate audio message.

9 Click the **General** tab.

The *New Entry Queue IVR Service - General* dialog box opens.
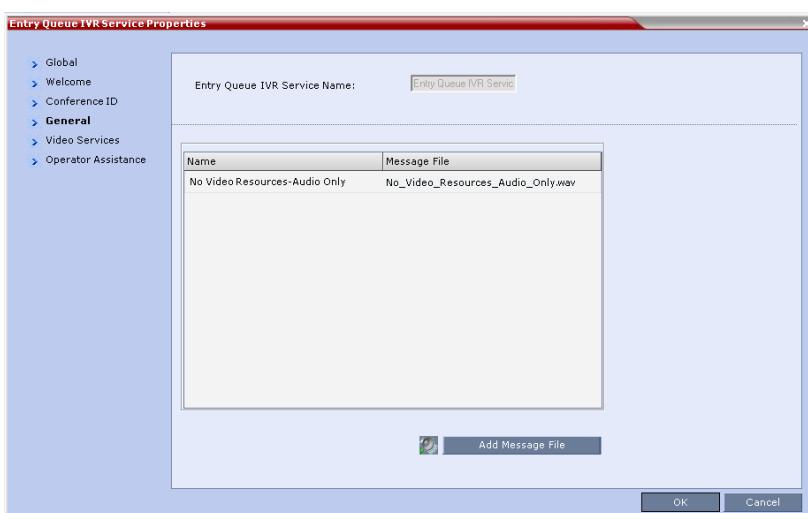
The administrator can enable an audio message that informs the participant of the lack of *Video Resources* in the *Collaboration Server* and that he/she is being connected as *Audio Only*. The message states: *All video resources are currently in use. Connecting using audio only*.

The following guidelines apply:

— The *IVR* message applies to video participants only. *Audio Only* participants will not receive the message.

— Only *H*.323 and *SIP* participants receive the audio message.

— The audio message is the first message after the call is connected, preceding all other *IVR* messages.

— The message is called *No Video Resources-Audio Only* and the message file (*.wav*) is called *No video resources audio only.wav*.

— The audio message must be added to the *Conference* and *Entry Queue IVR Services* separately.

— The IVR message can be enabled/disabled by the administrator using the **ENABLE_ NO_VIDEO_RESOURCES_ AUDIO_ONLY_MESSAGE** *System Flag* in *system.cfg*.

  Possible values: **YES / NO,** default: **YES**

If you wish to modify the flag value, the flag must be added to the *System Configuration* file. For more information see the "*Modifying System Flags*" on page **20-1**.

10 Enter the message *Name* and *Message File* name for the *Audio Only* message:

— Message *Name*: **No Video Resources-Audio Only**

— *Message File* name: **No_Video_Resources_Audio_Only.wav**

11 Click the **Video Services** tab.
The *New Entry Queue IVR Service - Video Services* dialog box opens.
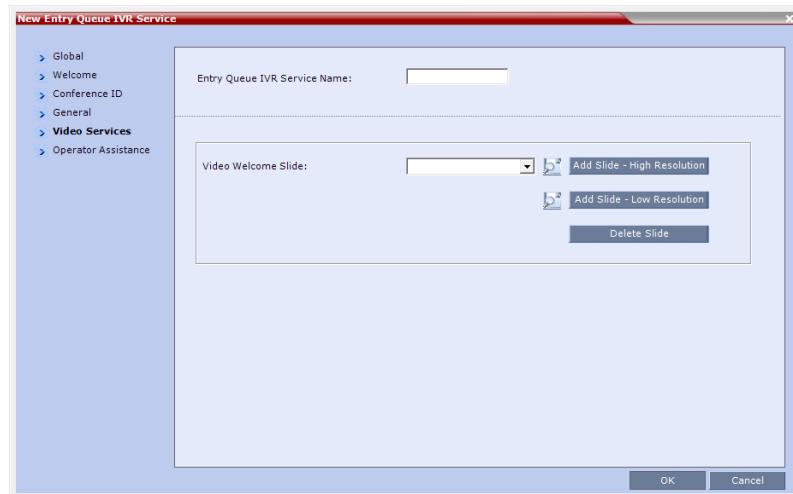
12 In the *Video Welcome Slide* list, select the video slide that will be displayed to participants connecting to the Entry Queue. The slide list includes the video slides that were previously uploaded to the MCU memory.

13 To view any slide, click the **Preview Slide** (image) button.

14 If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the:

— **Add Slide - Low Resolution** button to upload a *Low Resolution Slide*.

— **Add Slide - High Resolution** button to upload a *High Resolution Slide*.

The *Install File* dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step **6** on page **15-8**.

> The video slide must be in a .jpg or .bmp file format. For more information, see "*Creating a Welcome Video Slide*" on page **15-30**.

15 Click the **Operator Assistance** tab.
The *Operator Assistance* dialog box opens.

16 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.

17 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for operator's assistance.

> If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the *Collaboration Server*.

18 Click **OK** to complete the Entry Queue Service definition.
The new Entry Queue IVR Service is added to the *IVR Services* list. For more information, see "*IVR Services List*" on page **15-1**.

Setting a Conference IVR Service or Entry Queue IVR Service as the Default Service

The first Conference IVR Service and Entry Queue IVR Service are automatically selected by default. The IVR Services (Conference and Entry Queue) shipped with the system are also set as default. If additional Conference IVR Services and Entry Queue IVR Services are defined, you can set another service as the default for each service type.

To select the default Conference IVR Service:

>> In the *IVR Services* list, select the Conference IVR Service to be defined as the default, and then click the **Set Default Conference IVR Service** (⊞) button.

Alternatively, in the *IVR Services* list, right-click the Conference IVR Service and then select *Set Default Conference IVR Service*.
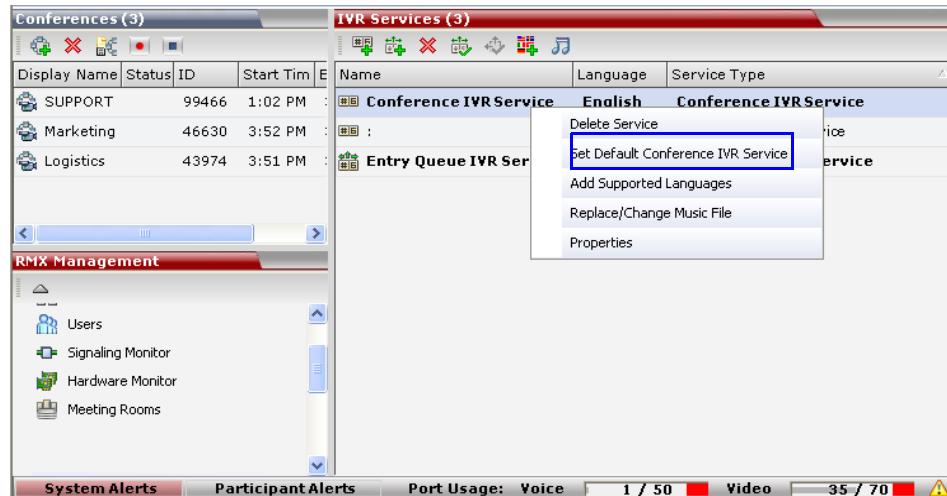
The IVR Service is displayed in bold, indicating that it is the current default service.

To select the Default Entry Queue IVR Service:

>>   In the *IVR Services* list, select the Entry Queue IVR Service to be defined as the default, and then click **Set Default Entry Queue IVR Service** (⊕) button.

Alternatively, in the *Conference IVR Services* list, right-click the Entry Queue IVR Service and then select *Set Default Entry Queue IVR Service*.
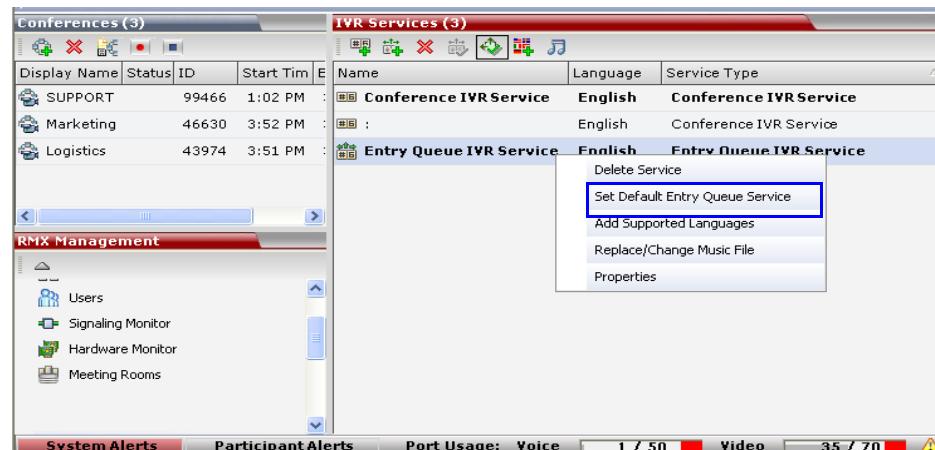
The default Entry Queue IVR Service is displayed in bold, indicating that it is the current default service.

Modifying the Conference or Entry Queue IVR Service Properties

You can modify the properties of an existing IVR Service, except the service name and language.

To modify the properties of an IVR Service:

1 In the *Collaboration Server Management* pane, click **IVR Services**.

2 In the *IVR Services* list, Click the IVR Service to modify.
For more information about the tabs and options of this dialog box, see "*Defining a New Conference IVR Service"* on page **15-6**.

3 Modify the required parameters or upload the required audio files.

4 Click **OK**.

Replacing the Music File

The *Collaboration Server* is shipped with a default music file that is played when participants are placed on hold, for example, while waiting for the chairperson to connect to the conference (if the conference requires a chairperson), or when a single participant is connected to the conference. You can replace the default music file with your own recorded music.

Music file guidelines:

- The file must be in *.wav format.
- Music length cannot exceed one hour.
- The music recording must be in the range of (-12dB) to (-9dB).

Adding a Music File

To replace the Music file:

1 In the *Collaboration Server Management* pane, click **IVR Services**.

2 In the *IVR Services* list toolbar, click the **Replace/Change Music File** (🎵) button. The *Install Music File* window opens.
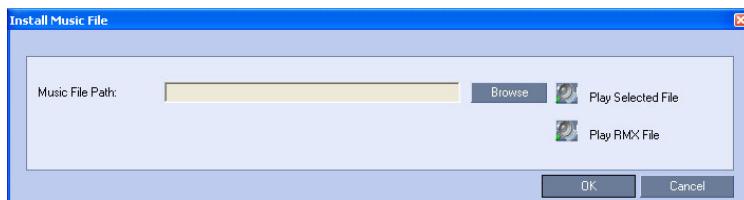
3 Click the **Browse** button to select the audio file (*.wav) to upload.

The *Open* dialog box opens.
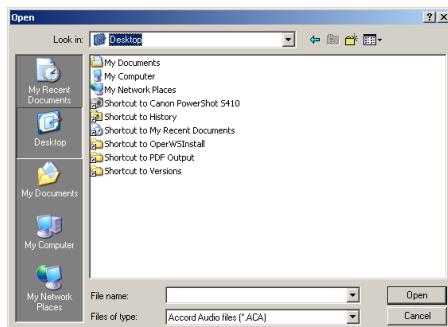
4 Select the appropriate audio *.wav file and then click the **Open** button. The selected file name is displayed in the *Install Music File* dialog box.

5 Optional. You can play the selected file by clicking the *Play* (🔊) button.

a Click **Play Selected File** to play a file on your computer.

b Click **Play *Collaboration Server* File** to play a file already uploaded on the *Collaboration Server*.

6 In the *Install Music File* dialog box, click **OK** to upload the file to the MCU. The new file replaces the previously uploaded file and this file is used for all background music played by the MCU.

Creating Audio Prompts and Video Slides

The *Collaboration Server* is shipped with default voice messages (in WAV format) and video slides that are used for the default IVR services. You can create your own video slides and record the voice messages for different languages or customize them to your needs.

Recording an Audio Message

To record audio messages, use any sound recording utility available in your computer or record them professionally in a recording studio. Make sure that recorded message can be saved as a Wave file (*.wav format) and that the recorded format settings are as defined in steps 4 and 5 on page **15-28**. The files are converted into the *Collaboration Server* internal format during the upload process.
This section describes the use of the Sound Recorder utility delivered with Windows 95/98/ 2000/XP.

To define the format settings for audio messages:

> • The format settings for audio messages need to be set only once. The settings will then be applied to any new audio messages recorded.
>
> • The utility or facility used to record audio messages must be capable of producing audio files with the formats and attributes as shown in the following procedure, namely, **PCM**, **16.000kHz, 16Bit, Mono**.
> Windows® XP® Sound Recorder is one of the utilities that can be used.

1 On your PC, click **Start > Programs > Accessories > Entertainment > Sound Recorder**.

The *Sound–Sound Recorder* dialog box opens.

2 To define the recording format, click **File > Properties**.

The *Properties for Sound* dialog box opens.

3 Click the **Convert Now** button.
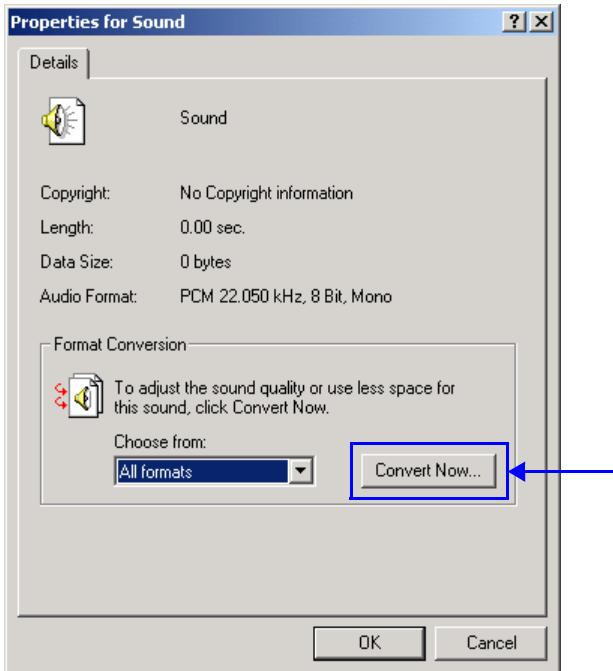
The *Sound Selection* dialog box opens.

4 In the *Format* field, select **PCM**.

5 In the *Attributes* list, select **16.000 kHz, 16Bit, Mono.**
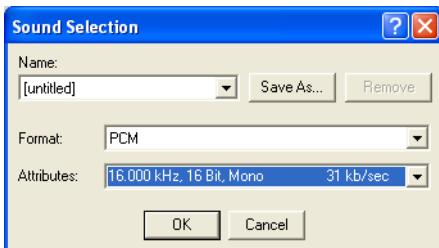
6 To save this format, click the **Save As** button.
The *Save As* dialog box opens.

7 Select the location where the format will reside, enter a name and then click **OK**.

The system returns to the *Sound Selection* dialog box.

8 Click **OK**.
The system returns to the *Properties for Sound* dialog box.

9 Click **OK**.
The system returns to the *Sound–Sound Recorder* dialog box. You are now ready to record your voice message.

To record a new audio message:

> Regardless of the recording utility you are using, verify that any new audio message recorded adheres to the following format settings: **16.000kHz, 16Bit, Mono**.

Make sure that a microphone or a sound input device is connected to your PC.

1   On your PC, click **Start > Programs > Accessories > Entertainment > Sound Recorder**.

    The *Sound–Sound Recorder* dialog box opens.

2   Click **File > New**.

3   Click the **Record** button.
    The system starts recording.

4   Start narrating the desired message.

> For all audio IVR messages, stop the recording anytime up to 3 minutes (which is the maximum duration allowed for an IVR voice message). If the message exceeds 3 minutes it will be rejected by the *Collaboration Server* unit.

5   Click the **Stop Recording** button.

6   Save the recorded message as a wave file, click **File > Save As**.

    The *Save As* dialog box opens.
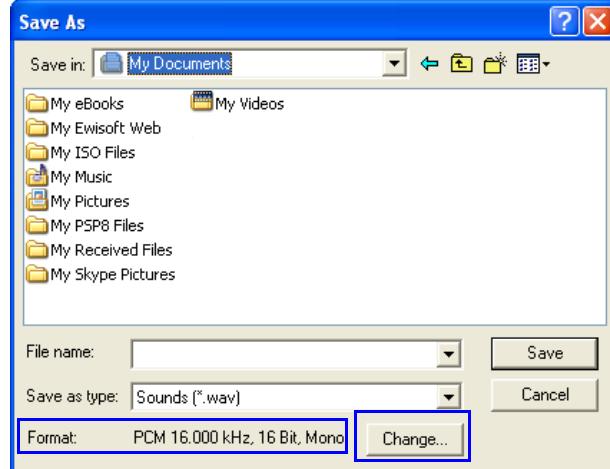
7   Verify that the *Format* reads: **PCM 16.000 kHz, 16Bit, Mono**. If the format is correct, continue with step 10. If the format is incorrect, click the **Change** button.

    The *Sound Selection* dialog box is displayed.
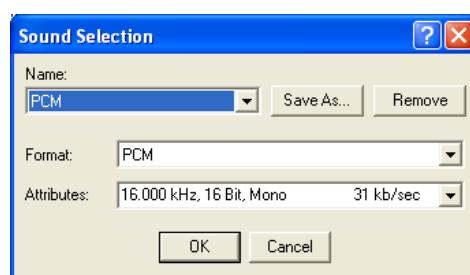
8   In the *Name* field, select the name of the format created in step 7 on page **15-28**.

9 Click **OK**.

The system returns to the *Save As* dialog box.

10 In the *Save in* field, select the directory where the file will be stored.

11 In the *Save as Type* field, select the ***.wav** file format.

12 In the *File name* box, type a name for the message file, and then click the **Save** button.

13 To record additional messages, repeat steps 1 to 10.

> To upload your recorded *.wav file to the *Collaboration Server*, see step 6 on page **15-8**.

Creating a Welcome Video Slide

The video slide is a still picture that can be created in any graphic application.

To create a welcome video slide:

1 Using any graphic application, save your image in either ***.jpg** or ***.bmp** file format.

2 For optimum quality, ensure that the image dimensions adhere to the *Collaboration Server* recommended values (width x height in pixels):

— 640 x 480

— 704 x 480

— 848 x 480

— 720 x 576

— 704 x 576

— 1024 x 576

— 960 x 720

— 1280 x 720

— 1440 x 1088

— 1920 x 1088

The *Collaboration Server* can accommodate small deviations from the recommended slide resolutions.

3 Save your file.

> Customized H.261 slides are not supported..

> If using a default Polycom slide, the slide's resolution will be as defined in the profile, i.e. SD, HD or CIF.
> If the display of the Welcome slide is cut in the upper area of the screen, change the settings of the endpoint's monitor to People "Stretch" instead of "Zoom".

> To upload your video slide to the *Collaboration Server*, see step 12 on page **15-22**.

Default IVR Prompts and Messages

The system is shipped with the following audio prompts and messages:

Table 15-12 Default IVR Messages

Message Type	Message Text	When Played	File Name
General Welcome Message	"Welcome to unified conferencing."	The participant enters the conference IVR queue	General_Welcome.wav
Chairperson Identifier Request	"For conference Chairperson Services, Press the Pound Key. All other participants please wait..."	The participant is asked to self-identify as the chairperson	Chairperson_ Identifier.wav
Request Chairperson Password	"Please enter the Conference Chairperson Password. Press the pound key when complete."	The participant is asked for the chairperson password	Chairperson_Password.wav
Retry Chairperson Password	"Invalid chairperson password. Please try again."	A participant enters an incorrect Chairperson password	Chairperson_ Password_Failure.wav
Request Password	"Please enter the conference password. Press the pound key when complete."	A participant is requested to enter the conference password	Conference_ Password.wav
Retry Password	"Invalid conference password. Please try again."	An incorrect conference password is entered	Retry_ Conference_ Password.wav
Request Digit	"Press any key to enter the conference."	A participant is requested to press any key	Request_Digit.wav
Request Billing Code	"Please enter the Billing code. Press the pound key when complete."	A participant is asked to enter a billing code	Billing_Code.wav
Requires Chairperson	"Please wait for the chairperson to join the conference."	A participant attempts to join a conference prior to the Chairperson joining	Requires Chairperson.wav
Chairperson Exit	"The chairperson has left the conference." **Note:** The *TERMINATE_CONF_AFTER_CHAIR_ DROPPED* flag must be enabled to play this message.	The chairperson has left the conference.	Chairperson_Exit.wav

Table 15-12 *Default IVR Messages (Continued)*

Message Type	Message Text	When Played	File Name
First to Join	"You are the first person to join the conference."	The first participant joins a conference	First to Join.wav
Mute All On	"All conference participants are now muted."	When all participants are muted by the operator or chairperson.	Mute_All_On.wav
Mute All Off	"All conference participants are now unmuted."	When all participants are unmuted by the operator or chairperson.	Mute_All_Off.wav
End Time Alert	"The conference is about to end."	The conference is about it end	End_Time_Alert.wav
Change Password Menu	"Press one to change conference password. Press two to change chairperson password. Press nine to exit the menu."	A participant requests a conference password change	Change_Password_ Menu.wav
Change Conference Password	"Please enter the new conference password. Press the pound key when complete."	A participant presses two in the *Change Password* IVR menu.	Change_ Conference_ Password.wav
Change Chairperson Password	"Please enter the new chairperson password. Press the pound key when complete."	A participant presses one in the *Change Password* IVR menu.	*Change_ Chairperson_ Password.wav*
Confirm Password Change	"Please re-enter the new password. Press the pound key when complete."	A participant enters a new conference or chairperson password	*Confirm_ Password_ Change.wav*
Change Password Failure	"The new password is invalid."	A participant enters an invalid password	*Change_ Password_ Failure.wav*
Password Changed Successfully	"The password has been successfully changed."	A participant has confirmed a password change	*Password_ Changed_ Successfully.wav*
Self Mute	"You are now muted."	A participant mutes his or her audio	*Self_Mute.wav*
Self Unmute	"You are no longer muted."	A participant unmutes his or her audio	*Self_Unmute.wav*

Table 15-12 *Default IVR Messages (Continued)*

Message Type	Message Text	When Played	File Name
Chairperson Help Menu	"The available touch-tone keypad actions are as follows: • To exit this menu press any key. • To request private assistance, press star, zero. • To request operator's assistance for the conference, press zero, zero. • To mute your line, press star, six. • To unmute your line, press pound, six."	A chairperson requests the chairperson help menu	*Chairperson_ Help_Menu.wav*
Participant Help Menu	"The available touch-tone keypad actions are as follows: • To exit this menu press any key. • To request private assistance, press star, zero. • To mute your line, press star, six. • To unmute your line, press pound, six.	A participant requests the participant help menu	*Participant_Help_Menu.wav*
Maximum Participants Exceeded	"The conference is full. You cannot join at this time."	A participant attempts to join a full conference	*Maximum_ Participants_ Exceeded.wav*
Request Conference NID	"Please enter your conference NID. Press the pound key when complete."		*Request_ Conference_NID.wav*
Retry Conference NID	"Invalid conference NID. Please try again."	A participant enters an invalid conference NID	*Retry_Conference_NID.wav*
Secured Conference	"The conference is now secured."	A chairperson or participant secures a conference	*Conference_Secured.wav*
Unsecured Conference	"The conference is now in an unsecured mode"	A chairperson or participant unsecures a conference	*Conference_Unsecured.wav*
Locked Conference	"Conference you are trying to join is locked"		*Conference_Locked.wav*
Conference Recording	"The conference is being recorded"		*Recording_ in_Progress.wav*
Conference Recording Failed	"The conference recording has failed"		*Recording_Failed.wav*
No Video Resources Audio Only.	"All video resources are currently in use. Connecting using audio only"		*No_Video_Resources_Audio_ Only.wav*

Volume Control of IVR Messages, Roll Call and Music

The volume of IVR music, and IVR messages is controlled by the following system flags:

- `IVR_MUSIC_VOLUME`
- `IVR_MESSAGE_VOLUME`

To control the volume of IVR music, Roll Call and messages:

>> Modify the values of the *System Flags* listed in Table 15-13 by clicking the menu **Setup > System Configuration**.

If these flags do not appear in the *System Flags* list, they must be manually added.

For more information see "*System Configuration Flags" on page 22-1.*

Table 15-13 *System Flags – IVR Volume Control*

Flag	Description
IVR_MUSIC_VOLUME	The volume of the IVR music played when a single participant is connected to the conference varies according to the value of this flag. Possible value range: 0-10 (Default: 2). 0 – disables playing the music 1 – lowest volume 10 – highest volume
IVR_MESSAGE_VOLUME	The volume of IVR messages varies according to the value of this flag. Possible value range: 0-10 (Default: 2). 0 – disables playing the IVR messages 1 – lowest volume 10 – highest volume **Note:** It is not recommended to disable IVR messages by setting the flag value to 0.

The following *System Flags* do not require an MCU reset:

- IVR_MESSAGE_VOLUME
- IVR_MUSIC_VOLUME

For all other flag changes, the MCU must be reset for the modified flag settings (including deletion) to take effect.

IP Network Services

To enable the Polycom RMX 1800 to function within IP network environments, network parameters must be defined for the *IP Network Services.*

The configuration dialog boxes for the IP network services are accessed via the *Collaboration Server Management* pane of the *Collaboration Server Web Client.*
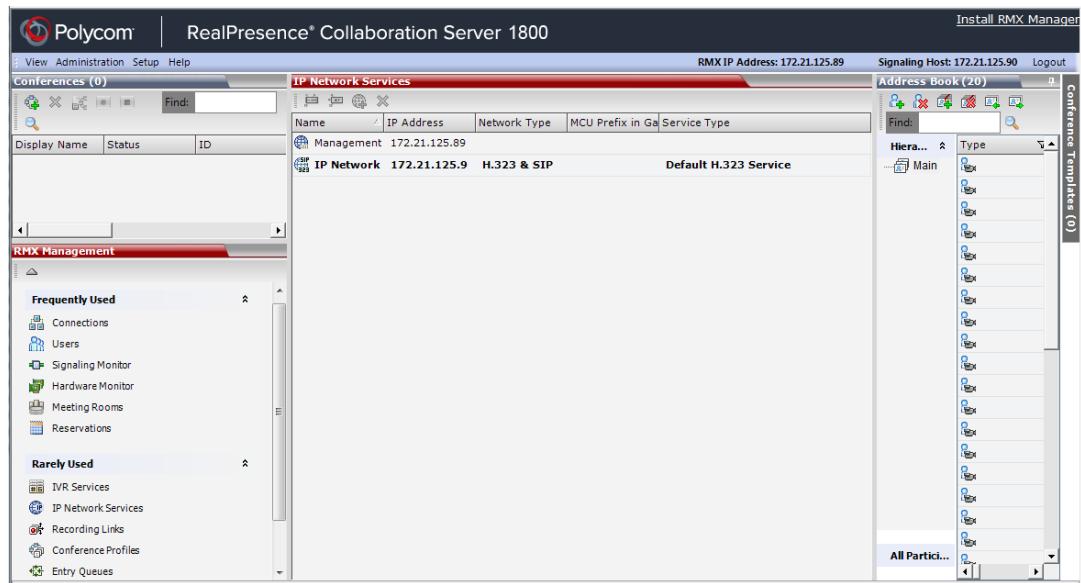
IP Network Services

Two *IP Services* are defined for the Collaboration Server:

• **Management Network**

• **Default IP Service (Conferencing Service)**

Dial in, dial out connections and Collaboration Server management are supported within IPv4 addressing environments.

Management Network (Primary)

The *Management Network* is used to control the Collaboration Server, mainly via the *RP Collaboration Server Web Client* application. The *Management Network* contains the network parameters, such as the IP address of the *Control Unit,* needed for connection between the Collaboration Server unit and the *RP Collaboration Server Web Client.* This IP address can be used by the administrator or service personnel to connect to the *Control Unit* should the MCU become corrupted or inaccessible.

During *First Time Power-up*, the *Management Network* parameters can be set either via a *USB memory stick* or by using a cable to create a private network.

For more information, see the*RMX™ 1800 Getting Started Guide*, "*Installing the RMX 1800"* on page **2-3** and *Appendix G* of this manual, "*Configuring Direct Connections to the Collaboration Server"* on page **F-1**.

Default IP Service (Conferencing Service - Media and signaling)

The *Default IP Service (media and signaling)* is used to configure and manage communications between the Collaboration Server and conferencing devices such as endpoints, gatekeepers, SIP servers, etc.

The *Default IP Service* contains parameters for:

- Signaling Host IP Address
- External conferencing devices

Calls from all external IP entities are made to the *Signaling Host,* which initiates call set-up.

Conferencing related definitions such as environment (H.323 or SIP) are also defined in this service.

Most of the *Default IP Service* is configured by the *Fast Configuration Wizard,* which runs automatically should the following occur:

- First time power-up.
- Deletion of the D*efault IP Service*, followed by a system reset.

For more information, see the *RMX™ 1800 Getting Started Guide, "Procedure 1: First-time Power-up"* on page **2-8**.

> Changes made to any of these parameters only take effect when the Collaboration Server is reset. An *Active Alarm* is created when changes made to the system have not yet been implemented and the MCU must be reset.

Modifying the Management Network

The *Management Network* parameters need to be modified if you want to:

- Connect directly to the Collaboration Server from a workstation
- Modify routes
- Modify DNS information

To view or modify the Management Network Service:

1 In the *RMX Management* pane, click the **IP Network Services** ( ) button.

2 In the *IP Network Services* list pane, double-click the **Management Network** ( ) entry.

The *Management Network Properties - IP* dialog box opens.
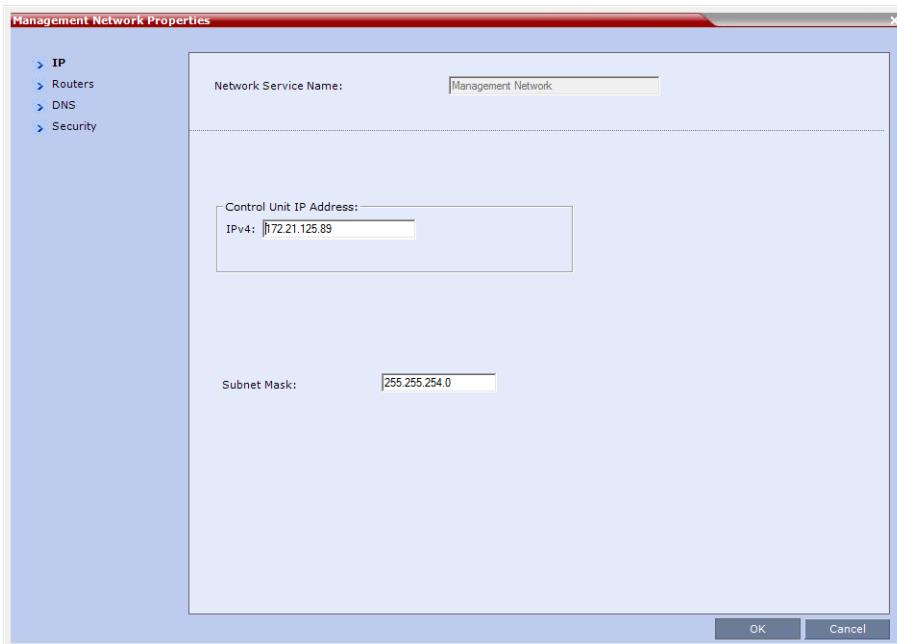
3   Modify the following fields:

Table 16-1   *Default Management Network Service – IP*

Field	Description	
Network Service Name	Displays the name of the Management Network. This name cannot be modified. **Note:** This field is displayed in all Management Network Properties tabs.	
Control Unit IP Address	IPv4	The IPv4 address of the Collaboration Server. This IP address is used by the *Collaboration Server Web Client* to connect to the Collaboration Server.
Subnet Mask	Enter the subnet mask of the Control Unit.	

4 Click the **Routers** tab.
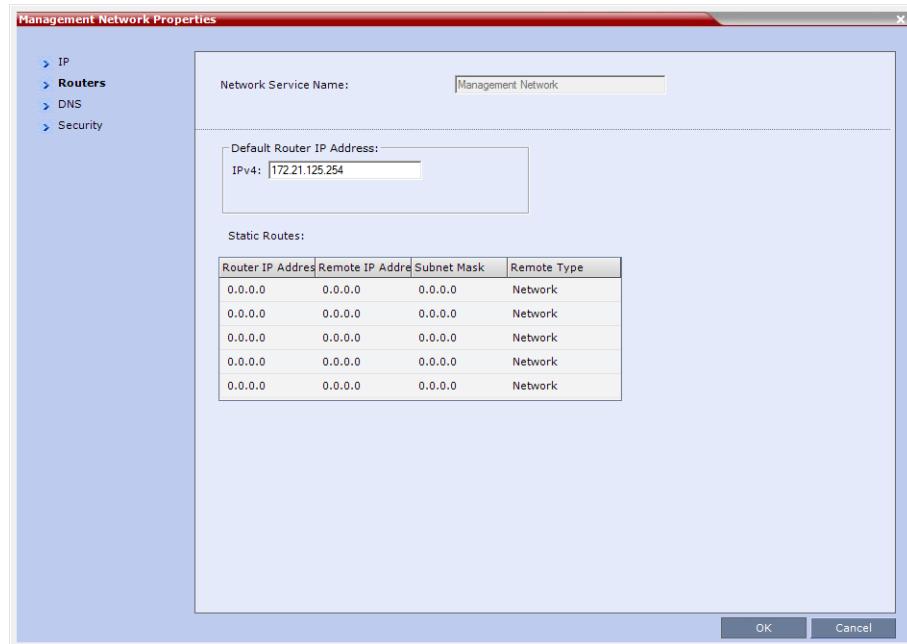
5 Modify the following fields:

Table 16-2 *Default Management Network Service – Routers*

Field	Description	
Default Router IP Address	IPv4	Enter the IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.

Table 16-2 *Default Management Network Service – Routers (Continued)*

Field		Description
Static Routes		The system uses *Static Routes* to search other networks for endpoint addresses that are not found on the local LAN. Up to five routers can be defined in addition to the Default Router. The order in which the routers appear in the list determines the order in which the system looks for the endpoints on the various networks. If the address is in the local subnet, no router is used. To define a static route (starting with the first), click the appropriate column and enter the required value.
	Router IP Address	Enter the IP address of the router.
	Remote IP Address	Enter the IP address of the entity to be reached outside the local network. The *Remote Type* determines whether this entity is a specific component (Host) or a network. • If Host is selected in the *Remote Type* field, enter the IP address of the endpoint. • If Network is selected in the *Remote Type* field, enter of the segment of the other network.
	Remote Subnet Mask	Enter the subnet mask of the remote network.
	Remote Type	Select the type of router connection: • **Network** – defines a connection to a router segment in another network. • **Host** – defines a direct connection to an endpoint found on another network.

6 Click the **DNS** tab.
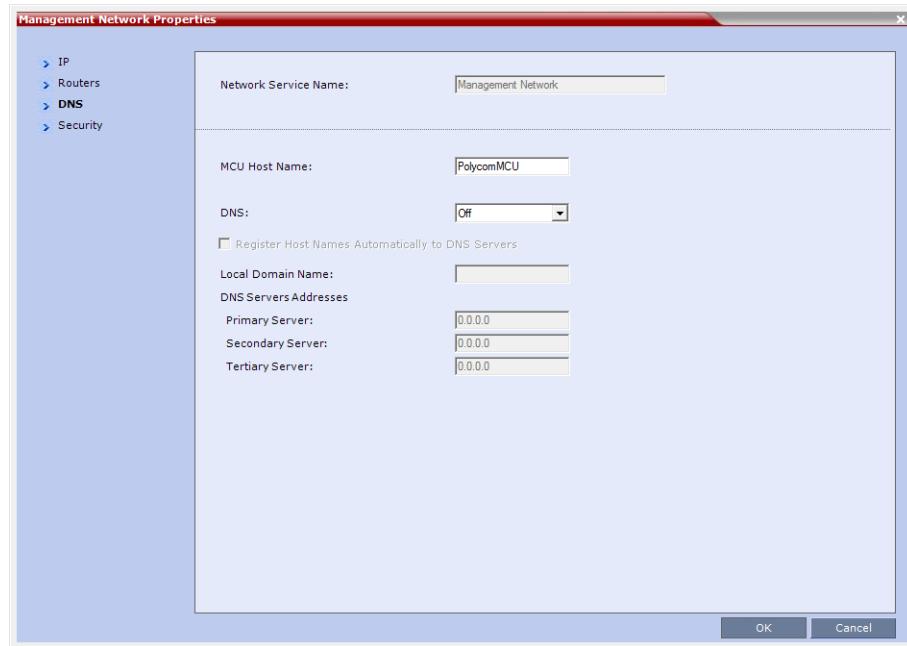
7 Modify the following fields:

Table 16-3 Default Management Network Service – DNS

Field	Description
MCU Host Name	Enter the name of the MCU on the network. Default name is PolycomMCU
DNS	Select: • **Off** – if DNS servers are not used in the network. • **Specify** – to enter the IP addresses of the DNS servers. **Note:** The IP address fields are enabled only if **Specify** is selected.
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host with the DNS server.
Local Domain Name	Enter the name of the domain where the MCU is installed.
DNS Servers Addresses:	
Primary Server	The static IP addresses of the DNS servers. A maximum of three servers can be defined.
Secondary Server	
Tertiary Server	

8   Click the **Security** tab.
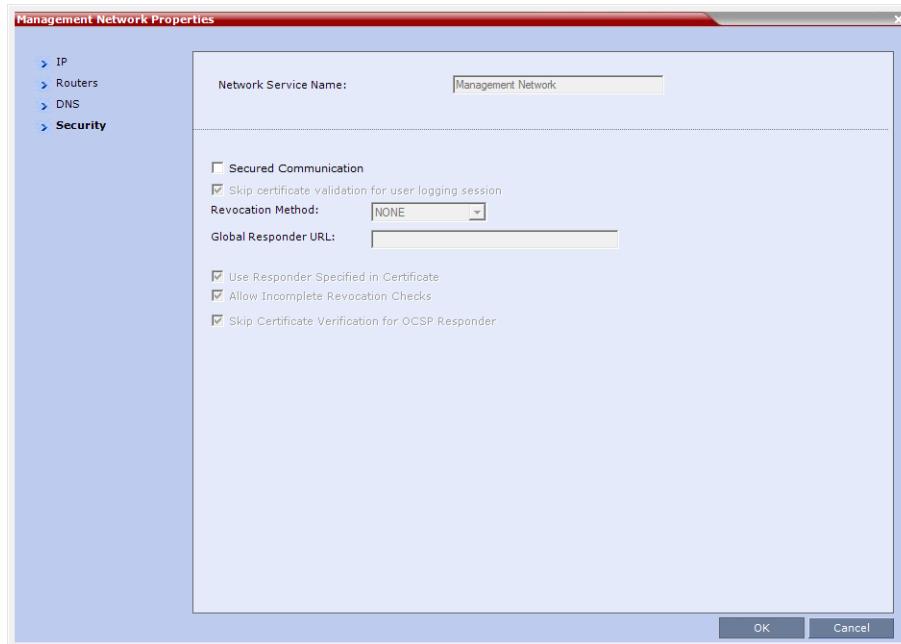
9   Modify the following fields:

Table 16-4 *Management Network Properties – Security Parameters*

Field	Description
Secured Communication	Select to enable Secured Communication. The Collaboration Server supports TLS 1.0 and SSL 3.0 (Secure Socket Layer). A SSL/TLS Certificate must installed on the Collaboration Server for this feature to be enabled.
Skip certificate validation for user logging session	Not supported with RealPresence Collaboration Server (RMX) 1500/2000/4000 .

10   Click **OK.**

11   If you have modified the *Management Network Properties*, reset the MCU.

Modifying the Default IP Network Service

The *Default IP Service* parameters need to be modified if you want to change the:

•   Network type that the Collaboration Server connects to
•   IP address of the Collaboration Server Signaling Host
•   Subnet mask of the Collaboration Server's IP cards
•   Gatekeeper parameters or add gatekeepers to the Alternate Gatekeepers list
•   SIP server parameters

Fast Configuration Wizard

The *Fast Configuration Wizard* enables you to configure the *Default IP Service*. It starts automatically if no *Default IP Network Service* is defined. This happens during *First Time Power-up*, before the service has been defined or if the *Default IP Service* has been deleted, followed by an Collaboration Server restart.

The *IP Management Service* tab in the *Fast Configuration Wizard* is enabled only if the factory default *Management IP addresses* were not modified.

If the *Fast Configuration Wizard* does not start automatically, the *Default IP Service* must be modified through the *IP Network Properties* dialog boxes.

To view or modify the Default IP Service:

1   In the *Collaboration Server Management* pane, click **IP Network Services** ( ).

2   In the *Network* list pane, double-click the **Default IP Service** (,   , or   ) entry.

The *Default IP Service - Networking IP* dialog box opens.
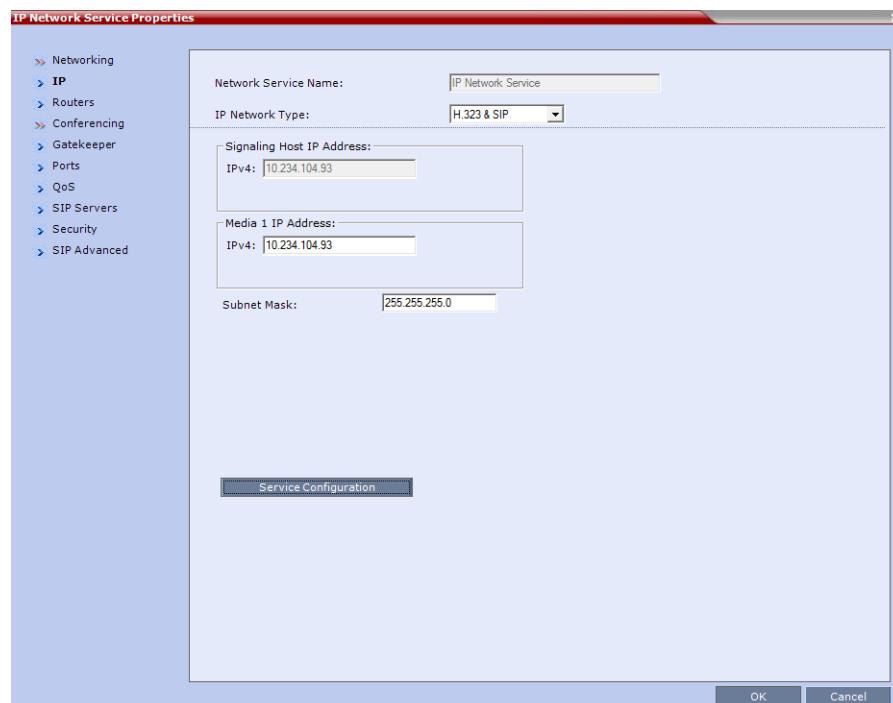
3   Modify the following fields:

Table 16-5 *Default IP Network Service – IP*

Field	Description
Network Service Name	The name *Default IP Service* is assigned to the IP Network Service by the Fast Configuration Wizard. This name can be changed. **Note:** This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.

Table 16-5 *Default IP Network Service – IP (Continued)*

Field	Description
IP Network Type	Displays the network type selected during the First Entry configuration. The Default IP Network icon indicates the selected environment. You can select: • **H.323:** For an H.323-only Network Service. • **SIP:** For a SIP-only Network Service. • **H.323 & SIP:** For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	On RMX 1800 this field is disabled as only one IP address is used for signaling and media transmission.
Media Card 1 IP Address	Enter the address to be used by IP endpoints when dialing in to the MCU.
Subnet Mask	Enter the subnet mask of the MCU. Default value: 255.255.255.0.

4 Click the **Routers** tab.
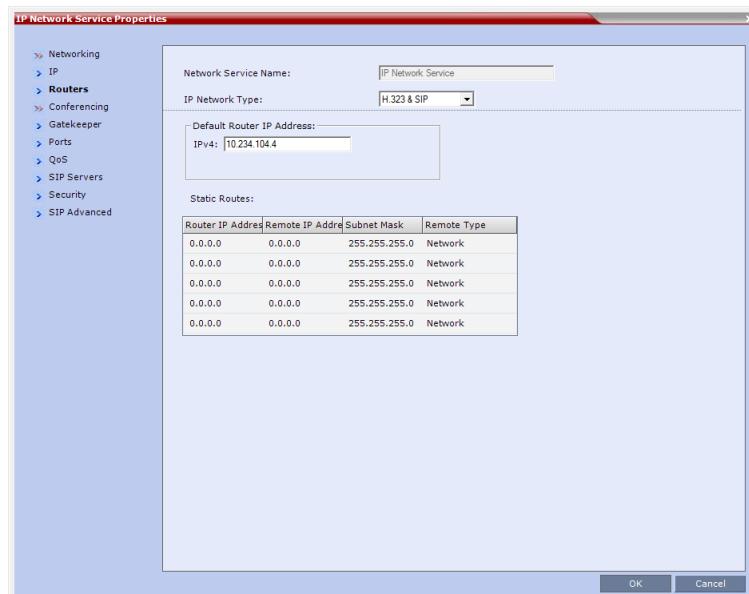
With the exception of *IP Network Type*, the field definitions of the *Routers* tab are the same as for the *Default Management Network.* For more information see page **16-4**.

5 **Optional.** Click the **DNS** tab.

Settings in this dialog box are relevant to *Multiple Network Services* only.

For more information see "*NAT (Network Address Translation) Traversal"* on page **16-23**.

6 Click the **Gatekeeper** tab.
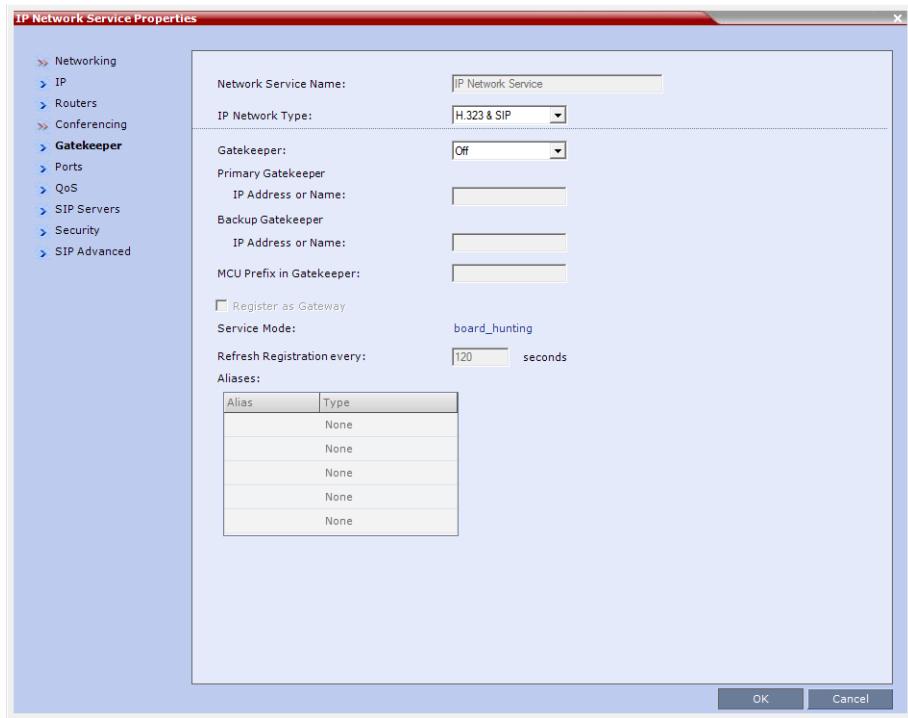
7 Modify the following fields:

Table 16-6 *Default IP Service – Conferencing – Gatekeeper Parameters*

Field	Description	
Gatekeeper	Select **Specify** to enable configuration of the gatekeeper IP address. When **Off** is selected, all gatekeeper options are disabled.	
Primary Gatekeeper IP Address or Name	Enter either the gatekeeper's host name as registered in the DNS or IP address.	
Backup Gatekeeper IP Address or Name	Enter the DNS host name or IP address of the gatekeeper used as a fallback gatekeeper used when the primary gatekeeper is not functioning properly.	
MCU Prefix in Gatekeeper	Enter the number with which this Network Service registers in the gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU.	
Register as Gateway	Select this check box if the Collaboration Server is to be seen as a gateway, for example, when using a Cisco gatekeeper.	

Table 16-6 *Default IP Service – Conferencing – Gatekeeper Parameters (Continued)*

Field	Description
Refresh Registration every __ seconds	The frequency with which the system informs the gatekeeper that it is active by re-sending the IP address and aliases of the system to the gatekeeper. If the system does not register within the defined time interval, the gatekeeper will not refer calls to the system until it re-registers. If set to 0, re-registration is disabled. **Note:** • It is recommended to use default settings. • This is a re-registration and not a 'keep alive' operation – an alternate gatekeeper address may be returned.
Aliases:	
Alias	The alias that identifies the Collaboration Server's Signaling Host within the network. Up to five aliases can be defined for each Collaboration Server. **Note:** When a gatekeeper is specified, at least one alias must be entered in the table. Additional aliases or prefixes may also be entered.
Type	The type defines the format in which the system alias is sent to the gatekeeper. Each alias can be of a different type: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * and #) • Email ID (email address format, e.g. abc@example.com) • Participant Number (digits 0-9, * and #) **Note:** Although all types are supported, the type of alias to be used depends on the gatekeeper's capabilities.

8   Click the **Ports** tab.

Settings in the *Ports* tab allow specific ports in the firewall to be allocated to multimedia conference calls.
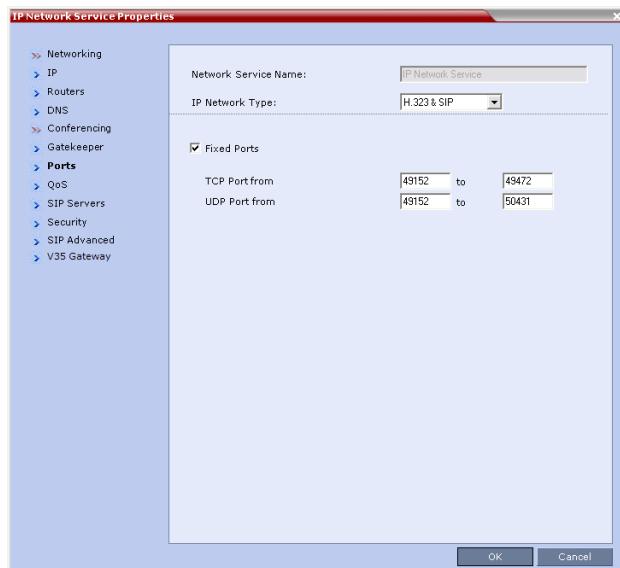
> Although you can define fixed ports, these ports are not implemented by the RealPresence Collaboration Server (RMX) 1500/2000/4000 .

The port range recommended by IANA (Internet Assigned Numbers Authority) is 49152 to 65535. The Collaboration Server uses this recommendation along with the number of licensed ports to calculate the port range.

9 Modify the following fields:

Table 16-7 Default IP Service – Conferencing – Ports Parameters

Field	Description
Fixed Ports	Leave this check box cleared if you are defining a Network Service for local calls that do not require configuring the firewall to accept calls from external entities. When cleared, the system uses the default port range and allocates 4 RTP and 4 RTCP ports for media channels (Audio, Video, Content and FECC). Click this check box to manually define the port ranges or to limit the number of ports to be left open.
TCP Port from - to	Displays the default settings for port numbers used for signaling and control. To modify the number of TCP ports, enter the first and last port numbers in the range. The number of ports is calculated as follows: Number of simultaneous calls x 2 ports (1 signaling + 1 control).

Table 16-7 *Default IP Service – Conferencing – Ports Parameters (Continued)*

Field	Description
UDP Port from - to	Displays the default settings for port numbers used for audio and video. To modify the number of UDP ports: Enter the first and last port numbers in the range, and the range must be **1024** ports.

If the network administrator does not specify an adequate port range, the system will accept the settings and issue a warning. Calls will be rejected when the Collaboration Server's ports are exceeded.

10 If required, click the **QoS** tab.
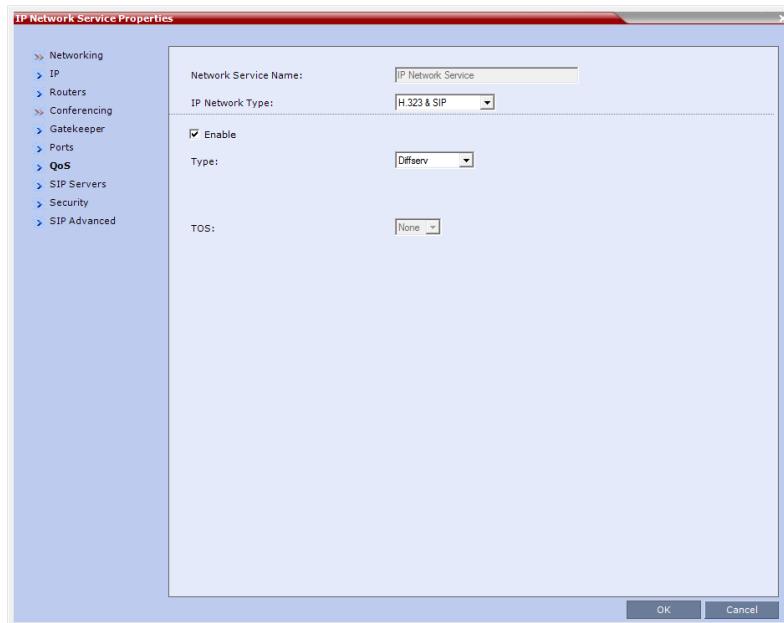
Quality of Service (QoS) is important when transmitting high bandwidth audio and video information. *QoS* can be measured and guaranteed in terms of:

• Average delay between packets

• Variation in delay (jitter)

• Transmission error rate

DiffServ and *Precedence* are the two *QoS* methods supported by the Collaboration Server. These methods differ in the way the packet's priority is encoded in the packet header.

The Collaboration Server's implementation of *QoS* is defined per Network Service, not per endpoint.

The routers must support QoS in order for IP packets to get higher priority.

11 View or modify the following fields:

Table 16-8 Default IP Service – Conferencing – QoS Parameters

Field	Description
Enable	Select to enable the configuration and use of the QoS settings. When un-checked, the values of the DSCP (Differentiated Services Code Point) bits in the IP packet headers are zero.

Type	DiffServ and Precedence are two methods for encoding packet priority. The priority set here for audio video and IP Signaling packets should match the priority set in the router.
	• **DiffServ:** Select when the network router uses DiffServ for priority encoding.
	  The default priorities for both audio and video packets is 0x88. These values are determined by the QOS_IP_VIDEO and QOS_IP_AUDIO flags in the *system.cfg* file.
	  The default priority for Signaling IP traffic is 0x00 and is determined by the QOS_IP_SIGNALING flag in the *system.cfg* file.
	For more information "*Modifying System Flags"* on page **20-1**.
	• **Precedence:** Select when the network router uses Precedence for priority encoding, or when you are not sure which method is used by the router. Precedence should be combined with None in the TOS field.
	  The default priority is 5 for audio and 4 for video packets.
	  Note: Precedence is the default mode as it is capable of providing priority services to all types of routers, as well as being currently the most common mechanism.

Audio / Video	You can prioritize audio and video IP packets to ensure that all participants in the conference hear and see each other clearly. Select the desired priority. The scale is from 0 to 5, where 0 is the lowest priority and 5 is the highest. The recommended priority is 4 for audio and 4 for video to ensure that the delay for both packet types is the same and that audio and video packets are synchronized and to ensure lip sync.
TOS	Select the type of Service (TOS) that defines optimization tagging for routing the conferences audio and video packets. • **Delay:** The recommended default for video conferencing; prioritized audio and video packets tagged with this definition are delivered with minimal delay (the throughput of IP packets minimizes the queue sequence and the delay between packets). • **None:** No optimization definition is applied. This is a compatibility mode in which routing is based on Precedence priority settings only. Select None if you do not know which standard your router supports.

12 Click the **SIP Servers** tab.
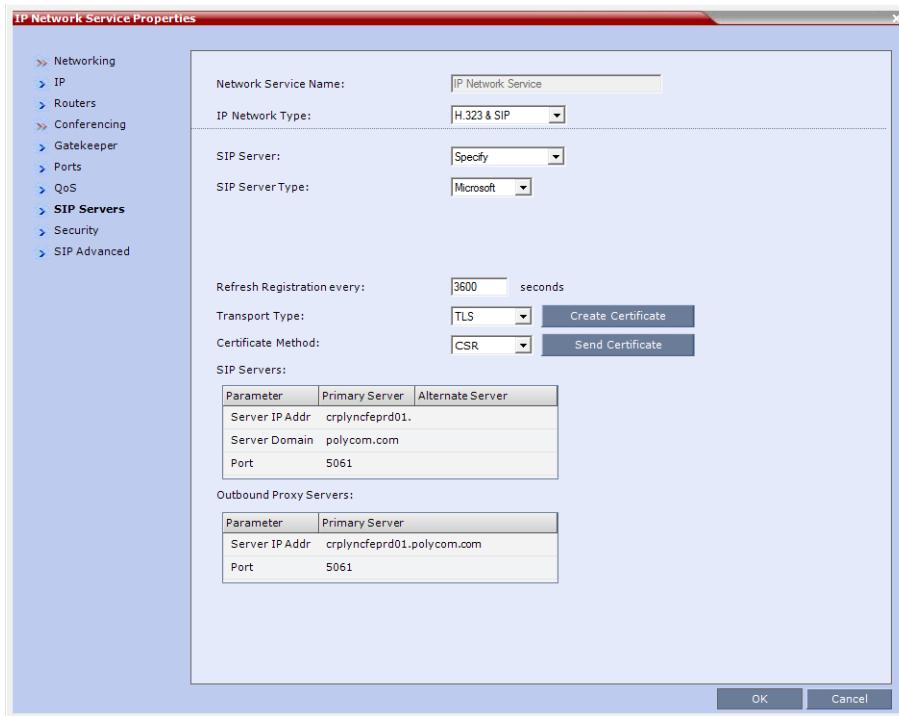
13 Modify the following fields:

Table 16-9 *Default IP Network Service – SIP Servers*

Field	Description
SIP Server	Select: • **Specify** – to manually configure SIP servers. • **Off** – if SIP servers are not present in the network.
Refresh Registration	This defines the time in seconds, in which the Collaboration Server refreshes it's registration on the SIP server. For example, if "3600" is entered the Collaboration Server will refresh it's registration on the SIP server every 3600 seconds.
Transport Type	Select the protocol that is used for signaling between the Collaboration Server and the SIP Server or the endpoints according to the protocol supported by the SIP Server: **UDP –** Select this option to use UDP for signaling. **TCP –** Select this option to use TCP for signaling. **TLS –** The *Signaling Host* listens on secured port 5061 only and all outgoing connections are established on secured connections. Calls from SIP clients or servers to non secured ports are rejected. The following protocols are supported: TLS 1.0, SSL 2.0 and SSL 3.0.

Table 16-9 Default IP Network Service – SIP Servers (Continued)

Field	Description
Create Certificate	This button is used to create a Certificate Request to be sent to a Certification Authority.
Certificate Method	Select the method for sending the Certificate to the Collaboration Server: • CSR • PEM/PFX
SIP Servers: Primary / Backup Server Parameter	
Server IP Address	Enter the IP address of the preferred SIP server. If a DNS is used, you can enter the SIP server name.
Server Domain Name	Enter the name of the domain that you are using for conferences, for example: `user_name@domain name` The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string. For example, when a call to `EQ1@polycom.com` reaches its outbound proxy, this proxy looks for the SIP server in the `polycom.com` domain, to which it will forward the call. When this call arrives at the SIP server in `polycom.com`, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.
Port	Enter the number of the TCP or UDP port used for listening. The port number must match the port number configured in the SIP server. Default port is 5060.
Outbound Proxy Servers: Primary / Alternate Server Parameter	
Server IP Address	By default, the Outbound Proxy Server is the same as the SIP Server. If they differ, modify the IP address of the Outbound Proxy and the listening port number (if required).
Port	Enter the port number the outbound proxy is listening to. The default port is 5060.

When updating the parameters of the SIP Server in the *IP Network Service - SIP Servers* dialog box, the Collaboration Server must be reset to implement the change.

14 Click the **Security** tab.
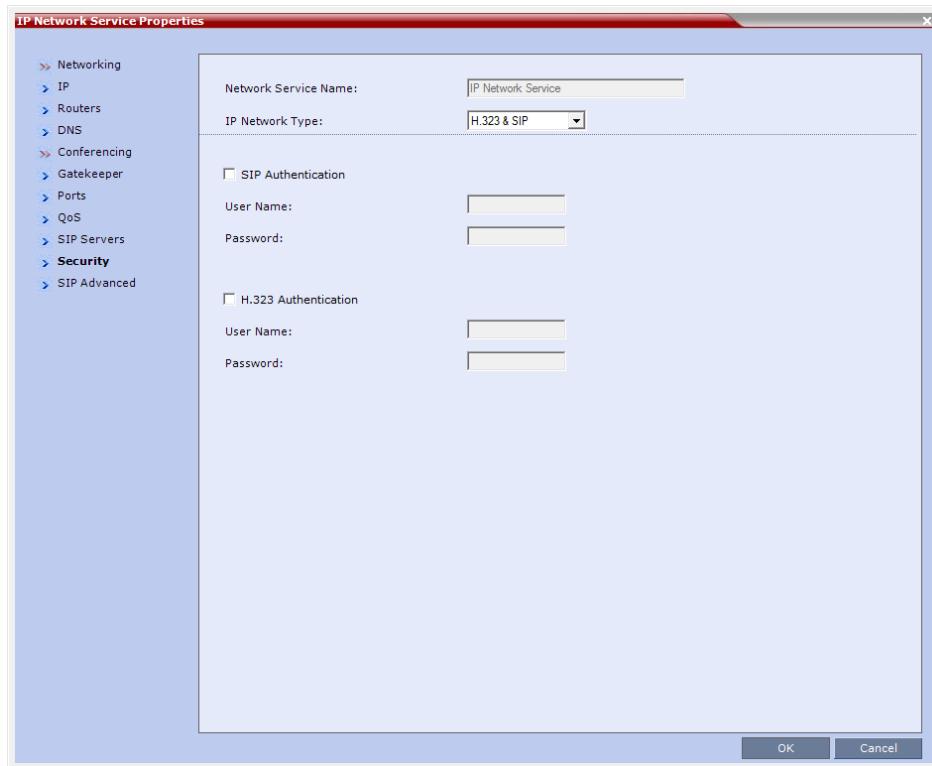
15 Modify the following fields:

Table 16-10 *Default IP Network Service – Security (SIP Digest)*

Field		Description	
SIP Authentication		Click this check box to enable SIP proxy authentication. Select this check box only if the authentication is enabled on the SIP proxy, to enable the Collaboration Server to register with the SIP proxy. If the authentication is enabled on the SIP proxy and disabled on the RMX, calls will fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the SIP proxy.	
	User Name	Enter the user name the Collaboration Server will use to authenticate itself with the SIP proxy. This name must be defined in the SIP proxy.	These fields can contain up to 20 ASCII characters.
	Password	Enter the password the Collaboration Server will use to authenticate itself with the gatekeeper. This password must be defined in the SIP proxy.	

Table 16-10 Default IP Network Service – Security (SIP Digest) (Continued)

Field		Description	
H.323 Authentication		Click this check box to enable H.323 server authentication. Select this check box only if the authentication is enabled on the gatekeeper, to enable the Collaboration Server to register with the gatekeeper. If the authentication is enabled on the gatekeeper and disabled on the RMX, calls will fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the gatekeeper.	
	User Name	Enter the user name the Collaboration Server will use to authenticate itself with the gatekeeper. This name must be defined in the gatekeeper.	These fields can contain up to 64 ASCII characters.
	Password	Enter the password the Collaboration Server will use to authenticate itself with the gatekeeper. This password must be defined in the gatekeeper.	

If the *Authentication User Name* and *Authentication Password* fields are left empty, the SIP Digest authentication request is rejected. For registration without authentication, the Collaboration Server must be registered as a trusted entity on the SIP server.

16 Click the **OK** button.

> When updating the parameters of the SIP Server in the *IP Network Service - SIP Servers* dialog box, the Collaboration Server must be reset to implement the change.

Ethernet Settings

In the Polycom RMX 1800, the automatically identified speed and transmit/receive mode of each LAN port used by the system can be manually modified if the specific switch requires it.

> Only the Management LAN interface is configurable.

To modify the automatic LAN port configuration:

1 On the Collaboration Server menu, click **Setup > Ethernet Settings**.

The *Ethernet Settings* dialog box opens.
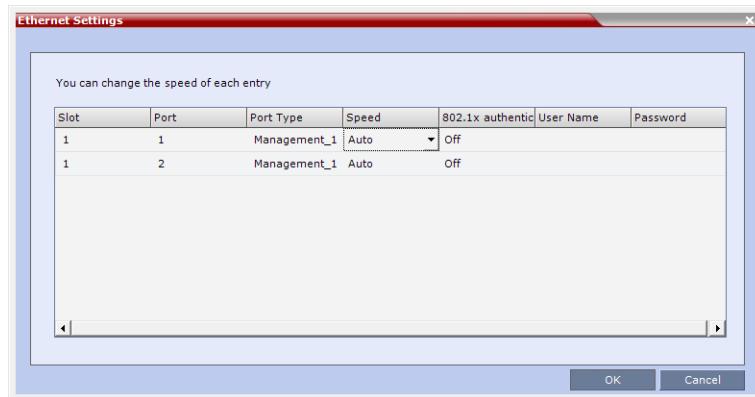
The Collaboration Server has 2 LAN ports. You can select the speed and transmit/receive mode manually for these ports.

2 In the *Speed* column, click the drop-down arrow of the table entry to modify and select the speed and the transmit/receive mode for each port:
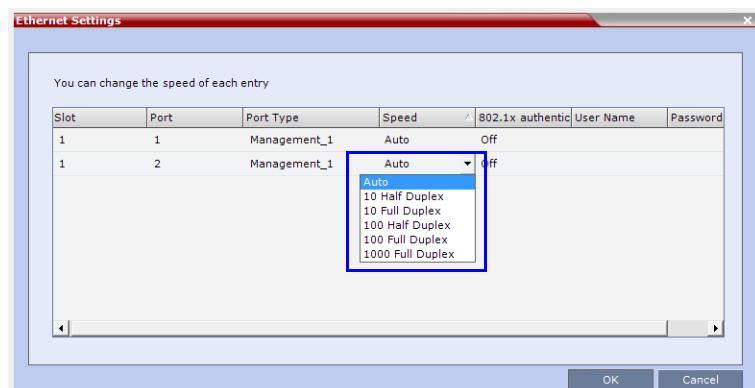
When **Auto** (default) is selected, the negotiation of speed and transmit/receive mode starts at 1000 Mbits/second Full Duplex, proceeding downward to 100 Mbits/second Half Duplex.

Note: To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended.

3 Click the **OK** button.

IP Network Monitoring

The *Signaling Monitor* is the Collaboration Server entity used for monitoring the status of external network entities such as the gatekeeper, DNS, SIP proxy and Outbound proxy and their interaction with the MCU.

To monitor signaling status:

1 In the *Collaboration Server Management* pane, click **Signaling Monitor** (⬛).

2 In the *Signaling Monitor* pane, double-click **Default IP Service**.

The *IP Network Services Properties – RMX CS IP* tab opens:
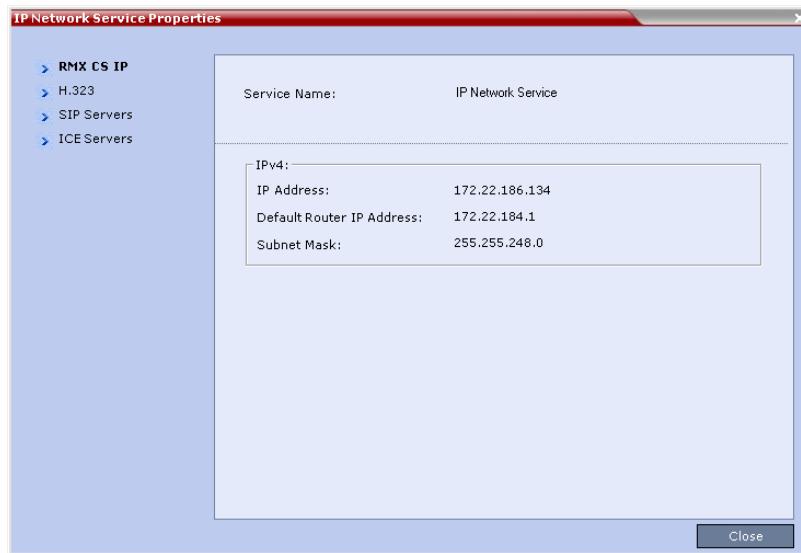
The *RMX CS IP* tab displays the following fields:

Table 16-11 IP Network Services Properties – RMX CS IP

Field	Description	
Service Name	The name assigned to the *IP Network Service* by the *Fast Configuration Wizard*. **Note:** This field is displayed in all tabs.	
IPv4	IP Address	
	Default Router IP Address	The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.
	Subnet Mask	The subnet mask of the MCU. Default value: 255.255.255.0.

3   Click the **H.323** tab.

The *H.323* tab displays the following fields:

Table 16-12 *IP Network Services Properties – H.323*

Field	Description
Connection State	The state of the connection between the Signaling Host and the gatekeeper: **Discovery** - The Signaling Host is attempting to locate the gatekeeper. **Registration** - The Signaling Host is in the process of registering with the gatekeeper. **Registered** - The Signaling Host is registered with the gatekeeper. **Not Registered** - The registration of the Signaling Host with the gatekeeper failed.
Registration Interval	The interval in seconds between the Signaling Host's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the gatekeeper during registration. The lesser value of the two is chosen.

	Role	**Active** - The active gatekeeper. **Backup** - The backup gatekeeper that can be used if the connection to the preferred gatekeeper fails.
	ID	The gatekeeper ID retrieved from the gatekeeper during the registration process.
	Name	The gatekeeper's host's name.
	IP Address	The gatekeeper's IP address.

4 Click the **SIP Servers** tab.
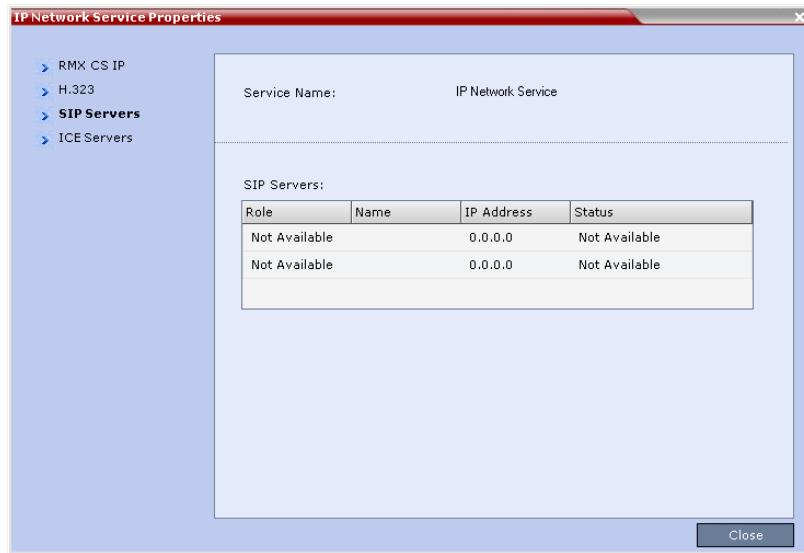
The *SIP Servers* tab displays the following fields:

Table 16-13 IP Network Services Properties – SIP Servers

Field	Description
Role	**Active** -The default SIP Server is used for SIP traffic. **Backup** -The SIP Server is used for SIP traffic if the preferred proxy fails.
Name	The name of the SIP Server.
IP Address	The SIP Server's IP address.
Status	The connection state between the SIP Server and the Signaling Host. **Not Available** - No SIP server is available. **Auto** - Gets information from DHCP, if used.

NAT (Network Address Translation) Traversal

NAT Traversal is a set of techniques enabling participants behind firewalls to connect to conferences, hosted on the Collaboration Server, remotely using the internet.

Session Border Controller (SBC)

All signaling and media for both SIP and H.323 will be routed through an *SBC*.
The following *SBC* environments are supported:

• *RealPresence Access Director (RPAD)* - a *Polycom SBC*

• *Acme Packet* - a 3rd party *SBC*

• *VBP* - *Polycom Video Border Proxy*

Deployment Architectures

The following *NAT Traversal* topologies are given as examples. Actual deployments will depend on user requirements and available infrastructure:

Remote Connection Using the Internet
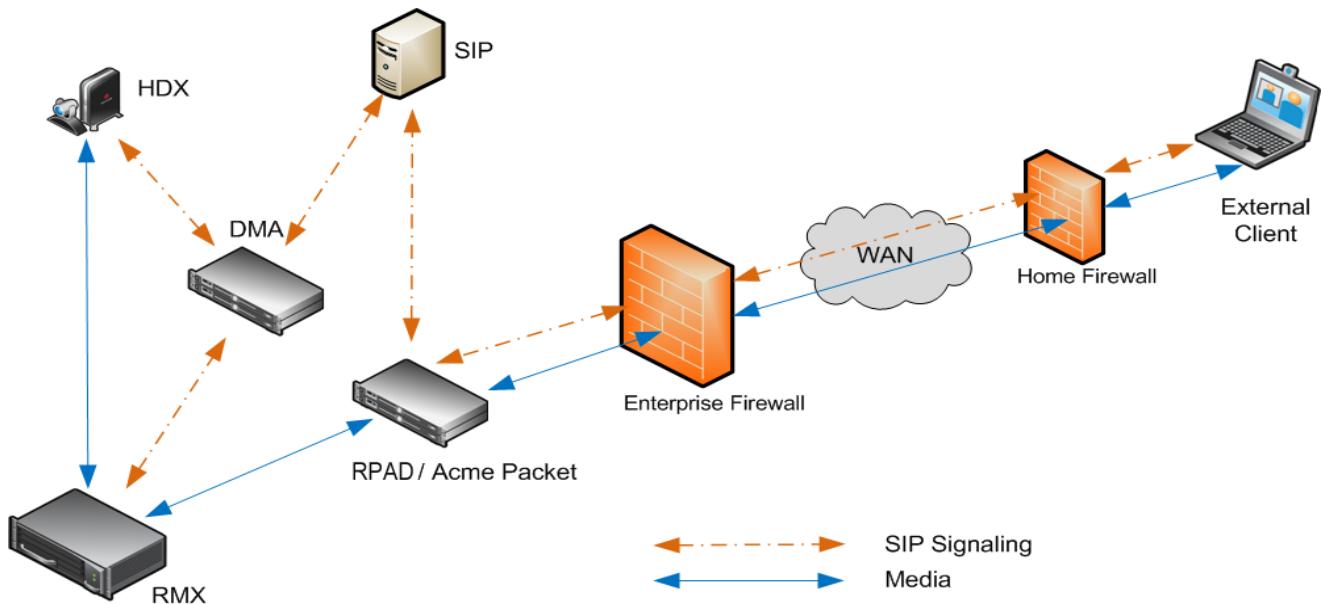
The following *Remote Connection* call flow options are supported:

Table 16-14 Remote Connection

Enterprise Client				CMA Client	
Environment	**Registered**	**SBC**		**Registered**	**Environment**
SIP / H.323	Yes	SAM / Acme Packet	⇄	Yes	*SIP*
SIP / H.323	No	SAM / Acme Packet	⇄	No	*SIP*

Table 16-14 Remote Connection (Continued)

Enterprise Client				CMA Client	
Environment	**Registered**	**SBC**		**Registered**	**Environment**
SIP / H.323	No	SAM Only	⇄	No	*H.323*

Business to Business Connections
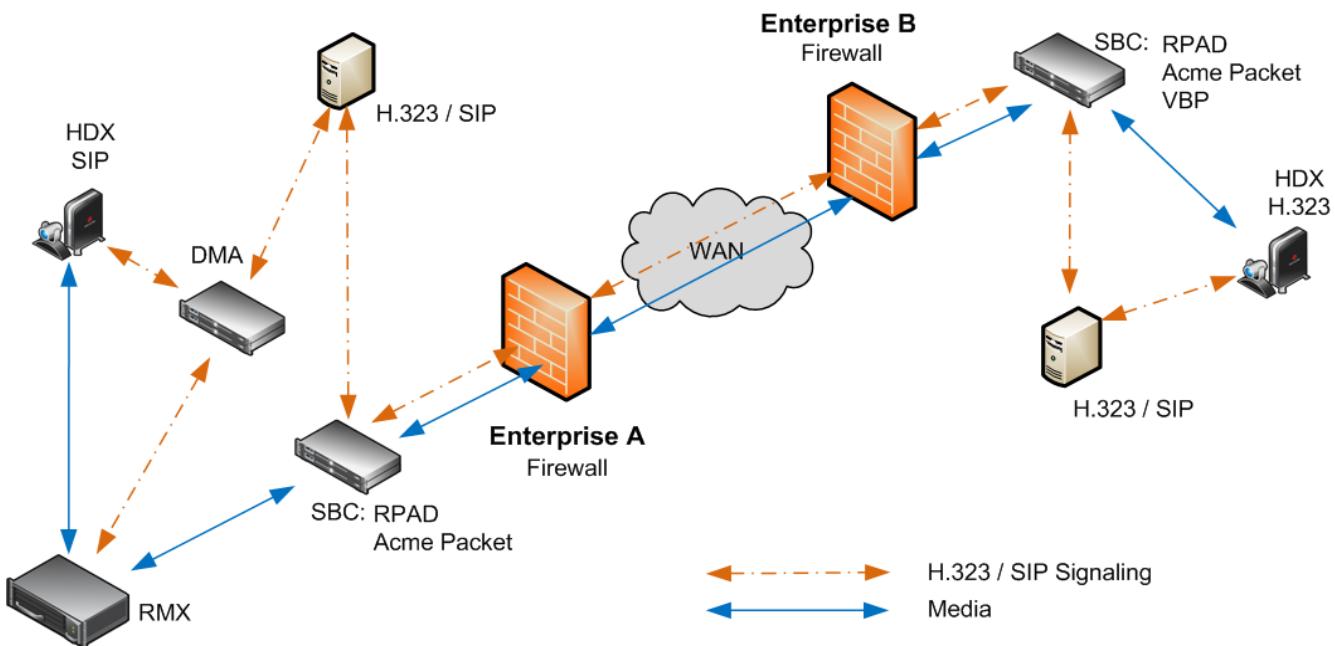
The following Business to Business connection call flow options are supported:

Table 16-15 Business to Business Connection

Enterprise A Client				Enterprise B Client		
Environment	**Registered**	**SBC**		**SBC**	**Registered**	**Environment**
H.323	Yes	RPAD	⇄	*RPAD*	Yes	*H.323*
H.323	Yes	RPAD	⇄	*VBP*	Yes	*H.323*
SIP	Yes	RPAD	⇄	*RPAD*	Yes	*H.323*
SIP	Yes	Acme Packet	⇄	Acme Packet	Yes	*H.323*

FW (Firewall) NAT Keep Alive

The Collaboration Server can be configured to send a *FW NAT keep alive* message at specific *Intervals* for the *RTP, UDP* and *BFCP* channels.

This is necessary because port mappings in the firewall are kept open only if there is network traffic in both directions. The firewall will only allow *UDP* packets into the network through ports that have been used to send packets out.

By default the Collaboration Server sends a *FW NAT Keep Alive* message every **30** seconds. As there is no traffic on the *Content* and *FECC* channels as a call begins, the firewall will not allow any incoming packets from the *Content* and *FECC* channels in until the Collaboration Server sends out the first of the *FW NAT Keep Alive* messages 30 seconds after the call starts.

If *Content* or *FECC* are required within the first 30 seconds of a call the *FW NAT Keep Alive Interval* should be modified to a lower value.

To enable and modify FW NAT Keep Alive:
FW NAT Keep Alive is enabled in the *New Profile - Advanced* dialog box.
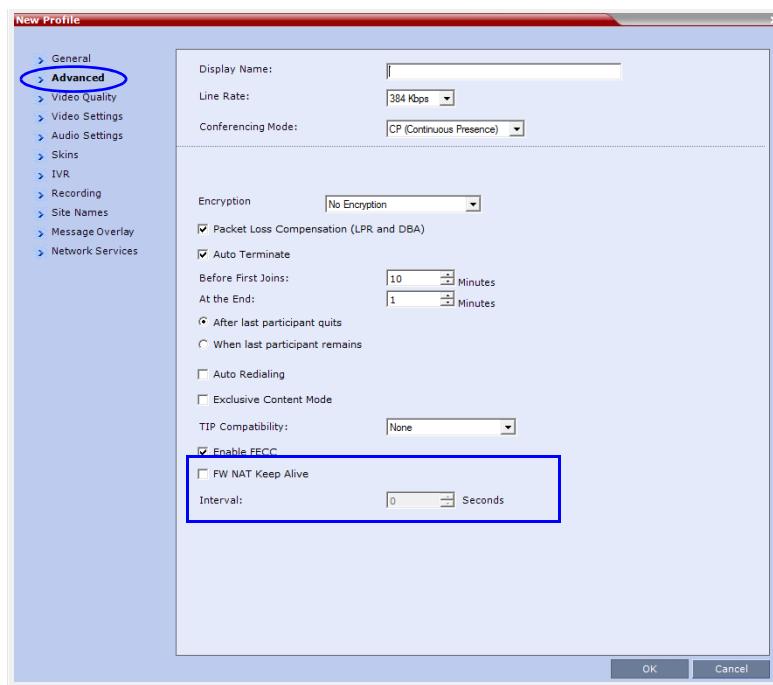
>> Select the *FW NAT Keep Alive* check box and if required, modify the *Interval* field within the range of **1 - 86400** seconds.

System Configuration in SBC environments

In an environment that includes *SAM* (a *Polycom SBC*), to ensure that a *RealPresence Mobile* endpoint can send content to a conference the value of the system flag **NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT** must be set to at least 3.

For more details on modifying the values of system flags, see "*Manually Adding and Deleting System Flags*" on page **20-10**

Polycom RMX 1800 Network Port Usage

The following table summarizes the port numbers and their usage in the Polycom RMX 1800:

Table 16-16 Collaboration Server Network Port Usage Summary

Connection Type	Port Number	Protocol	Description	Configurable
HTTP	80	TCP	Management between the Collaboration Server and *RP Collaboration Server Web Client*.	No
HTTPS	443	TCP	Secured Management between the Collaboration Server and *RP Collaboration Server Web Client*.	No
DNS	53	TCP	Domain name server.	Can be disabled in the IP Network Service.
DHCP	68	TCP	Dynamic Host Configuration Protocol.	Can be disabled in the IP Network Service.
SSH	22	TCP	Secured shell. It is the Collaboration Server terminal.	No
NTP	123	UDP	Network Time Protocol. Enables access to a time server on the network.	No
H.323 GK RAS	1719	UDP	Gatekeeper RAS messages traffic.	No
H.323 Q.931	1720 - incoming; 49152-59999 - outgoing	TCP	H.323 Q.931 call signaling. Each outgoing call has a separate port. The port for each outgoing call is allocated dynamically.	Yes - for outgoing calls only. It is configured in the Fixed Ports section of the IP service.
H.323 H.245	49152 - 59999	TCP	H.245 control. Each outgoing call has a separate port. The port for each outgoing call is allocated dynamically. It can be avoided by tunneling.	Yes - for outgoing calls only. It is configured in the Fixed Ports section of the IP service.
SIP server	5060 60000	UDP, TCP	Connection to the SIP Server. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.

Table 16-16 Collaboration Server Network Port Usage Summary (Continued)

Connection Type	Port Number	Protocol	Description	Configurable
Alternative SIP server	5060 60000	UDP, TCP	Connection to the alternate SIP Server. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
SIP Outbound proxy	5060 60000	UDP, TCP	Connection to the SIP outbound proxy. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
Alternative SIP Outbound proxy	5060 60000	UDP, TCP	Connection to the alternate SIP outbound proxy. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
SIP-TLS	60002	TCP	Required for Binary Floor Control Protocol (BFCP) functionality for SIP People+Content content sharing.	No - ,port is not opened if SIP People+Content is disabled.
RTP	49152 - 59999	UDP	RTP media packets. The ports are dynamically allocated.	Yes - It is configured in the Fixed Ports section of the IP service.
RTCP	49152 - 59999	UDP	RTP control. The ports are dynamically allocated.	Yes - It is configured in the Fixed Ports section of the IP service.
SIP -TLS	5061	TCP	SIP -TLS for SIP server, alternate SIP server, outbound proxy and alternate outbound proxy.	No

LAN Redundancy

LAN redundancy enables the redundant LAN port connection to automatically replace the failed port by using another physical connection and NIC (Network Interface Card). When a LAN port fails, IP network traffic failure is averted and network or endpoints disconnections do not occur. When LAN redundancy is enabled, by default, LAN 1 is the active port and LAN 2 is its backup.

Requirements

LAN redundancy is disabled by default. However, you can change its availability by setting the LAN_REDUNDANCY system flag.

> You cannot enable LAN Redundancy and Multiple Network Services at the same time. That is, if **MULTIPLE_SERVICES** is set as **YES** in the *System Flags*, you must changes its value to **NO** before you can set **LAN_REDUNDANCY** as **YES**.

Media, Signaling and Management Redundancy

On the Polycom RMX 1800, for Media, Signaling and Management Redundancy, you must set **LAN_REDUNDANCY** system flag to **YES**.

To enable LAN redundancy:

1   Make sure the **LAN_REDUNDANCY** system flag is set to **YES.**

   LAN_REDUNDANCY is set as **NO** by default, and is hidden in the *System Flags* list.

   To make sure **LAN_REDUNDANCY** is set as **YES**, do the following:

   a   On the RMX menu, click **Setup > System Configuration > System Configuration**.

      The *System Flags* dialog box opens.

   b   Select **MULTIPLE_SERVICES** and make sure it's value is **NO**. If not, click **Edit Flag** and change its value to **NO**.

   a   Select **LAN_REDUNDANCY** and make sure it's value is **YES**. If not**,** click **Edit Flag** and change its value to **YES.**

      If you cannot find **LAN_REDUNDANCY** in *System Flags* dialog box, click **New Flag** to add it, and set its value as **YES**.

2   Click **Close** to exit the **System Flags** window.

3   When prompted to reset the MCU, click **Yes**.

Hardware Monitor Indications

When LAN Redundancy is enabled on the Collaboration Server, LAN 1 port is *Active.* With LAN redundancy, when LAN LEDs are lit they indicate that a physical connection of the

cables is present but does not indicate their activity status. In the *Hardware Monitor* pane the *Lan List* displays the Collaboration Server LAN ports together with their *Status* indication.

RealPresence Collaboration Server 1800 Lan List (2)						
Slot	Port	Type	Status	802.1x status	802.1x method	802.1x failure
	0	LAN 1	Active	Not Configure	Off	Off
	0	LAN 2	Inactive	Not Configure	Off	Off

Table 16-17 RMX 1800 LAN LED Indications

Status	Description
Active	The LAN port cable is connected.
Inactive	The LAN port cable is not connected.
Standby	The LAN Redundancy option is enabled and this LAN port is the redundant and in standby mode. In case of failure, this port becomes active.

Multiple Network Services

Media, signaling and management networks can be logically separated on the Polycom RMX 1800 system to provide enhanced security. This addresses the requirement in an organization that different groups of participants be supported on different networks. For example, some participants may be internal to the organization while others are external.

Maximum two IP network Services can be defined for a Polycom RMX 1800 system.

Each conference on the Collaboration Server can host participants from the different IP Network networks simultaneously.

The following figure shows the network topology with two different media and signaling networks and one Management network connected to the Polycom RMX 1800 system.
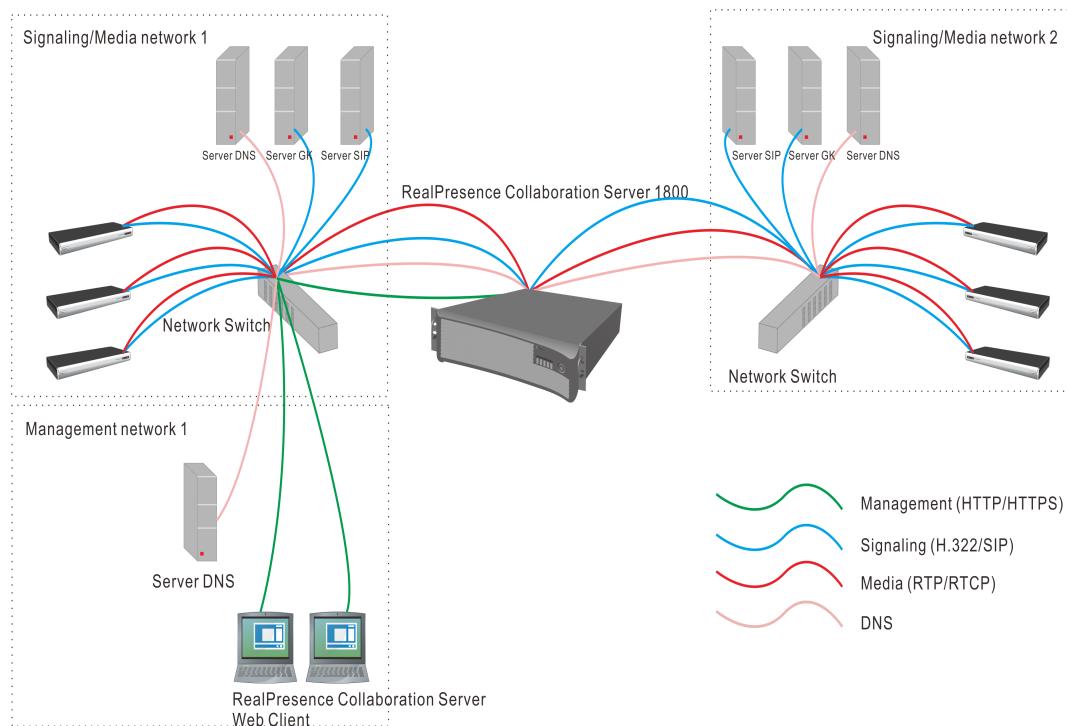
Figure 16-1 Polycom RMX 1800 - Multiple Network Topology Sample

Guidelines

- On the Polycom RMX 1800 system, when Multiple Network Services option is enabled, the two network services must be configured to different subnets.

- Participants on different networks can connect to the same conference with full audio, video and content capabilities.

- Traffic on one network does not influence or affect the traffic on other networks connected to the same MCU. If one network fails, it will not affect the traffic in the other connected networks.

- Maximum two network services and one management service can be defined.

- Participants are associated with a Network Service and use its resources as follows:
  — Dial-in participants - according to the network used to place the call and connect to the Collaboration Server.
  — Dial-out participant - according to the Network Service selected during the participant properties definition or during conference definition, according to the Network Service selected as default.
- Recording Links use the default Network Service to connect to conferences, therefore the recording system must be defined on the default network to enable the recording.

Resource Allocation and Capacity

The Video and Voice Port usage are reflected in the port gauges displayed on the Collaboration Server management application's main screen. However, the port gauges do not reflect the resource availability per Network Service.

Flexible Resource Allocation Mode

On the Polycom RMX 1800 system with two *Network Services* defined, the resources of the two Network Services are not split between the network services. In such a case, resources are used per their availability by both Network Services equally.

Using Multiple Network Service

Multiple Services is enabled by licence and must be purchased for the system.

Follow these steps to use Multiple Network Service:

1 Enable Multiple Services and disable LAN Redundancy.
2 Add the required IP Network Services to accommodate the networks connected to the Collaboration Server unit.
3 Select a Network Service to act as default for dial out calls for which the Network Service was not selected.

   Place several calls and run conferences to ensure that the system is configured correctly.

Enabling Multiple Network Service

You must set the system flags **MULTIPLE_SERVICES** to **YES** and **LAN_REDUNDANCY** to **NO** before you can enable Multiple Network Service**.**

To change system flags for use with Multiple Network Service:

1 On the RMX menu, click **Setup > System Configuration > System Configuration**.

   The *System Flags* dialog box opens.
2 Select **MULTIPLE_SERVICES** and select **Edit Flag**.
3 In the **New Value** field, change the value to **YES**, and then click **OK**.
4 Check the value of the flag **LAN_REDUNDANCY**. If its value is **YES**, click **Edit Flag** and change its value to **NO**.

   If you cannot find the flag **LAN_REDUNDANCY** in the *System Flags* list, do the following:

   a Click **New Flag**.
   b In the **New Flag** field, enter **LAN_REDUNDANCY**.
   c In the **Value field**, enter **NO**.
   d Click **OK**.

5 Click **Close** to exit the **System Flags** window.

6 When prompted to reset the MCU, click **Yes**.

Defining New IP Network Service

Use this procedure to define Network Services in addition to the Network Service already defined during first entry installation and configuration.

To add new/additional Network Services:

1 In the *Device Management* pane, click **IP Network Services** ( ).

2 In the *Network Services* list toolbar, click the   **Add Network Service** button.

The *New IP Service - Networking IP* dialog box opens.

3 Define the following fields:

Table 16-18 IP Network Service - IP Parameters

Field	Description
Network Service Name	Enter the IP Network Service name. **Note:** This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.
IP Network Type	Select the IP Network environment. You can select: • **H.323:** For an H.323-only Network Service. • **SIP:** For a SIP-only Network Service. • **H.323 & SIP:** For an integrated IP Service. Both H.323 and SIP participants can connect to the Collaboration Server using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	Enter the address to be used by IP endpoints when dialing into the Collaboration Server using this Network Service. Dial out calls of participants to whom this network service will be assigned are initiated from this address. This address is used to register the Collaboration Server with a Gatekeeper or a SIP Proxy server residing on this network. **Note:** The Signaling network shares the same IP address with the Media 2 IP address and is not editable.
Media 1 IP Address	Reserved for existing IP network Service. **Note**: DO NOT change this IP address here.
Media 2 IP Address	Enter the IP address for media network of the new IP network service.
Subnet Mask	Enter the subnet mask of the Collaboration Server in that network service. Default value: 255.255.255.0.

4 **Optional.** Some system flags can be defined per Network Service, depending on the network environment.
To modify these flags, click the **Service Configuration** button.

The *Service Configuration* dialog box opens.
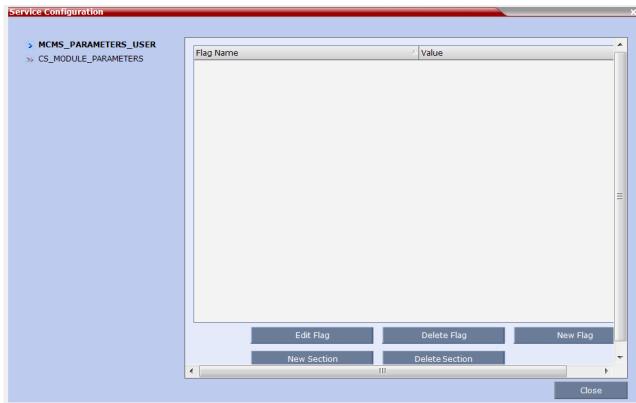
All the flags must be manually added to this dialog box. For a detailed description of the flags and how to add them, see "*Manually Adding and Deleting System Flags"* on page **20-10**.

> Flags defined per Network Service override their general definition in the System Configuration.

5 Click the **Routers** tab.

6 Define the routers used in this network and that are other than the routers defined in the Management Network. The field definitions of the *Routers* tab are the same as for the *Default Management Network.*

7 Click the **Gatekeeper** tab.

8 Define the *Primary* and *Alternate Gatekeepers* and at least one **Alias** for this network Service. The field definitions of the *Gatekeeper* tab are the same as for the *Default IP Network Service.*

> In *Multiple Services* mode, an Alias must be defined for the specified gatekeeper.

9 **Optional.** Click the **Ports** tab.

Settings in the *Ports* tab allow specific ports in the firewall to be allocated to multimedia conference calls. If required, defined the ports to be used multimedia conference calls handled by this Network Service. The field definitions of the *Ports* tab are the same as for the *Default IP Network Service.*

10 If required, click the **QoS** tab.

The Collaboration Server's implementation of *QoS* is defined per Network Service, not per endpoint.

> The routers must support QoS in order for IP packets to get higher priority.

The field definitions of the *QoS* tab are the same as for the *Default IP Network Service.*

11 Click the **SIP Servers** tab.

12 Define the *Primary* and *Alternate SIP Server* for this network Service.

The field definitions of the *SIP Servers* tab are the same as for the *Default IP Network Service*.

13 Click the **Security** tab.

The field definitions of the *Security* tab are the same as for the *Default IP Network Service*.

14 Click the **OK** button.
The new Network Service is added to the *IP Network Services* list pane.

Setting a Network Service as Default

The default Network Service is used when no Network Service is selected for the following:

* Dial out participants
* Reserving resources for participants when starting an ongoing conference

In addition, the Signaling Host IP address and the MCU Prefix in GK displayed on the *RP Collaboration Server Web Client* main screen are taken from the default H.323 Network Service.

One IP Network Service can be defined as default for H.323 connections and another Network Service as default for SIP connections. If the IP Network Service supports both H.323 and SIP connections, you can set the same Network Service as default for both H.323 and SIP, or for H.323-only or for SIP-only.

To designate an IP Network Service as the default IP Network Service:

1 In the *Device Management* pane, click **IP Network Services** ( ).

2 In the *Network Services* list pane right-click the IP Network Service to be set as the default, and then click **Set Default H.323 Service,** or **Set Default SIP** Service.

To set this IP Network Service for both H.323 and SIP connections, repeat step 2 and select the option you need.

The following icons are used to indicate the default IP Network Service type:

Table 16-19 Default IP Network Service Icons

Icon	Description
	This Network Service supports both SIP and H.323 connections and is designated as default for both SIP and H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for SIP connections.
	This Network Service supports only H.323 connections and is set as default for H.323 connections.
	This Network Service supports only SIP connections and is set as default for SIP connections.

Ethernet Settings

The Polycom RMX 1800 is set to automatically identify the speed and transmit/receive mode of each LAN ports. These port settings can be manually configured if the specific switch requires it, via the **Ethernet Settings**. For more details, see "*IP Network Monitoring*" on page **16-19**.

> The Port numbers displayed in the dialog box do not reflect the physical Port numbers as labeled on the RealPresence Collaboration Server (RMX) 1500/2000/4000 system.

Signaling Host IP Address and MCU Prefix in GK Indications

The *RP Collaboration Server Web Client* displays the *Signaling Host IP Address* and *MCU Prefix in GK* parameters as defined in the **Default H.323 Network Servic**e.

Conference Profile

Registration of conferencing entities such as ongoing conferences, Meeting Rooms, Entry Queues and SIP Factories with SIP servers is done per conferencing entity. This allows better control on the number of entities that register with each SIP server by selecting for each of the conferencing entities whether it will register with the SIP server.

The registration is defined in the *Conference Profile - Network Services* tab.
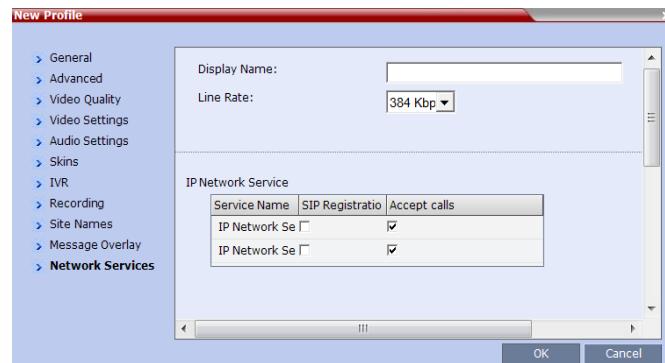
In the *IP Network Services* table, the system lists all the defined Network Services (one or two depending on the system configuration).

- To register the conferencing entity to which this profile is assigned to a Network Service, in the *Registration* column click the check box of that Network Service.

- You can also prevent dial in participants from connecting to that conferencing entities when connecting via a Network Service.
  In the *Accept Calls* column, clear the check box of the Network Service from which calls cannot connect to the conference.

Hardware Monitor

The Hardware Monitor pane includes the status of the LAN ports.

Lan List (2)			
Slot	Port	Type	Status
🔌	0	LAN 1	Active
🔌	0	LAN 2	Inactive

Signaling Monitor

The Signaling Monitor pane includes the list of the IP Network Services defined in the system (up to two in the Polycom RMX 1800 system). Double-clicking a Network Service, displays it properties and status.

Name	IP Address	Router	Subnet Mask
IP Network	172.21.125.2	172.21.125.254	255.255.254.0
IP Network	192.168.100.	192.168.100.254	255.255.255.0

Multiple service Signaling Monitor (2)

Conferencing

Each conference on the Collaboration Server can host participants from the different IP Network networks simultaneously.

Defining Dial Out Participants

When defining dial out participants, you can select the Network Service to place the call according to the network to which the endpoint pertains. If the endpoint is located on a network other than the selected network, the participant will not be able to connect.

If no Network is selected, the system uses the IP Network Service selected for reserving the conference resources, and if none is set for the conference it uses the Network Service set as default.

The IP Network Service is selected in the *New Participant - Advanced* dialog box.
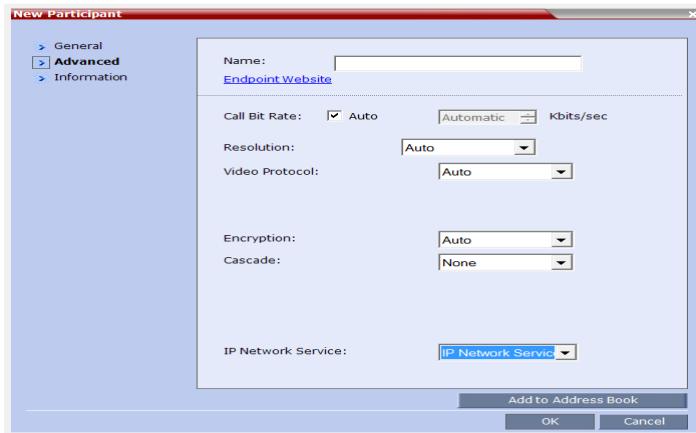
Reserving Video Resources for a Conference

When defining a new ongoing conference or a conference reservation, you can select the Network Service that will be used to reserve the required resources. If no Network Service is selected, the default Network Service is used. Therefore, make sure that not all conferences are reserving resources from the same Network Service, otherwise you may run out of resources for that Network Service.

The IP Network Service is selected in the *New Conference/New Meeting Room/New Reservation - General* dialog box.
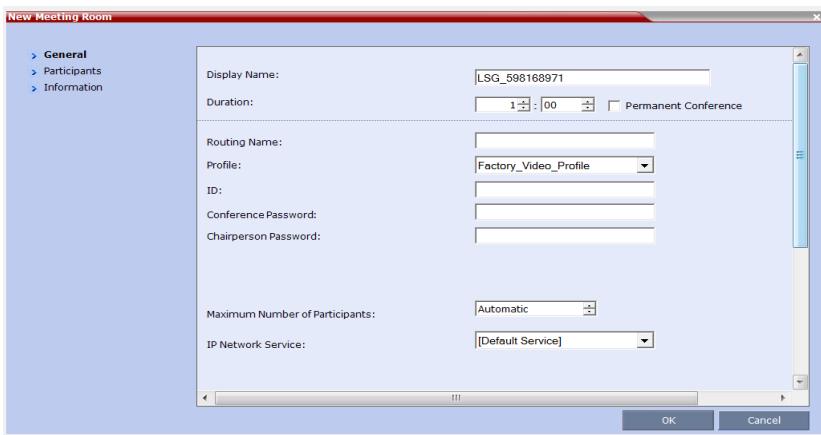
Monitoring Conferences

The *Conference Properties - Network Services* dialog box shows for each Network Service with which Network Service's SIP proxy the conference should be registered and if the dial in call will be connected to the conference.

In the *Participant* pane, a new column - *Service Name* was added, indicating the name of Network Service used for the participant's connection.

Resource Report

The *Resource Report* displays the resource usage in total and per Network Service in a table format. The Resources per Service table provides the actual information on resource usage and availability per network Service and provides an accurate snapshot of resources usage in the system.

You can select the graph to display: select either **Totals** (default) or the Network Service.
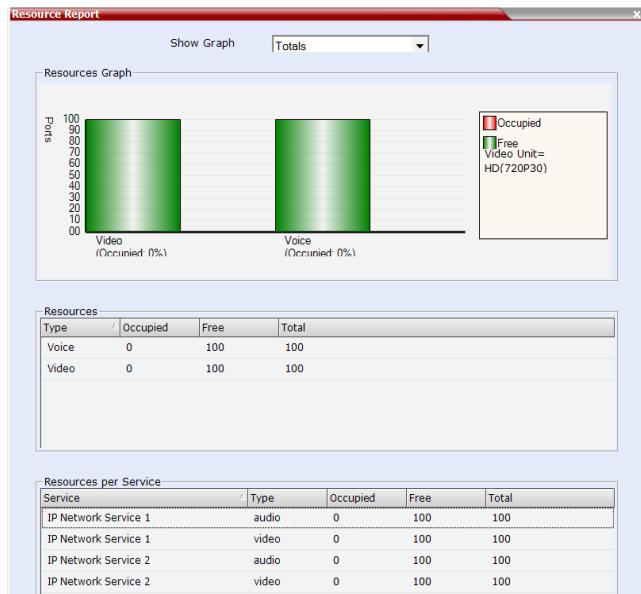
Port Gauge Indications

The port Gauges displays the total resource usage for the Collaboration Server and not per Network Service. Therefore, it may not be an accurate representation of the availability of resources for conferencing, as one Network Service may run out of available resources while another Network Service may have all of it resources available. In such a case, the port gauges may show that half of the system resources are available for conferencing, while calls via the Network Service with no available resources will fail to connect.

17

The Call Detail Record (CDR) Utility

The Call Detail Record (CDR) utility enables you to view summary information about conferences, and retrieve full conference information and archive it to a file. The file can be used to produce reports or can be exported to external billing programs.

> The value of the fields that support Unicode values, such as the info fields, will be stored in the CDR file in UTF8. The application that reads the CDR must support Unicode.

The *Collaboration Server* can store details of up to 2000 conferences. When this number is exceeded, the system overwrites conferences, starting with the earliest conference. To save the conferences' information, their data must be retrieved and archived. The frequency with which the archiving should be performed depends on the volume of conferences run by the MCU.

The *Collaboration Server* displays Active Alarms before overwriting the older files, enabling the users to backup the older files before they are deleted.

The display of Active Alarms is controlled by the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS System Flag.

If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file storage capacity limit, an Active Alarm is created: "Backup of CDR files is required".

Each conference is a separate record in the MCU memory. Each conference is archived as a separate file. Each conference CDR file contains general information about the conference, such as the conference name, ID, start time and duration, as well as information about events occurring during the conference, such as adding a new participant, disconnecting a participant or extending the length of the conference.

The CDR File

CDR File Formats

The conference CDR records can be retrieved and archived in the following two formats:

- **Unformatted data** – Unformatted CDR files contain multiple records in "raw data" format. The first record in each file contains general conference data. The remaining records contain event data, one record for each event. Each record contains field values separated by commas. This data can be transferred to an external program such as Microsoft Excel© for billing purposes.

The following is a sample of an unformatted CDR file:

Conference summary record

Event code

Event records

Figure 17-1 *Unformatted CDR File*

*   **Formatted text** – Formatted CDR files contain multiple sections. The first section in each file contains general conference data. The remaining sections contain event data, one section for each event. Each field value is displayed in a separate line, together with its name. This data can be used to generate a summary report for a conference

> The field names and values in the formatted file will appear in the language being used for the *Collaboration Server Web Client* user interface at the time when the CDR information is retrieved.

The following is an example of a formatted CDR file:

General conference section

Event heading

Event section

Figure 17-2 *Formatted CDR File*

Multi-Part CDR Files

By default, the maximum CDR (Call Data Record) file size is limited to 1MB. When a *CDR* file reaches a size of 1MB the file is saved and further call data recording is stopped and the additional data is lost.

The *Collaboration Server* can be configured to keep recording the data in multiple CDR file set of 1MB each. *Multi-Part CDR* ensures that conference call data from long duration or permanent conferences is recorded and not lost.

Guidelines

- *Multi-Part CDR* is enabled by setting the value of the **ENABLE_MULTI_PART_CDR** *System Flag* to **YES**.

  The flag's default value is **NO**.

  When the flag value is **NO,** *CDR* file size is limited to one file of 1MB and further call data recording is stopped.

  To modify the default setting, the flag must be manually added to the *System Configuration*. For more information see, "*Modifying System Flags*" on page **20-1**.

- If the flag value is set to **YES**, when a *CDR* file reaches 1MB, an additional *CDR* file is created and added to the *CDR* file set for that conference.

- If the flag value is changed from **YES** to **NO** (or visa versa) all existing *CDR* files are retained.

CDR File Contents

The general conference section or record contains information such as the Routing Name and ID, and the conference starting date and time.

The event sections or records contain an event type heading or event type code, followed by event data. For example, an event type may be that a participant connects to the conference, and the event data will list the date and time the participant connects to the conference, the participant name and ID, and the participant capabilities used to connect to the conference.

To enable compatibility for applications that written for the MGC family, the *Collaboration Server* CDR file structure is based on the MGC CDR file structure.

The unformatted and formatted text files contain basically the same information. The following differences should be noted between the contents of the unformatted and formatted text files:

- In many cases a formatted text file field contains a textual value, whereas the equivalent unformatted file field contains a numeric value that represents the textual value.

- For reading clarity, in a few instances, a single field in the unformatted file is converted to multiple fields in the formatted text file, and in other cases, multiple fields in the unformatted file are combined into one field in the formatted file.

- To enable compatibility between MGC CDR files and *Collaboration Server* CDR files, the unformatted file contains fields that were applicable to the MGC MCUs, but are not supported by the *Collaboration Server* MCUs. These fields are omitted from the formatted text file.

Appendix C: "*CDR Fields - Unformatted File*" on page **C-1**, contains a full list of the events, fields and values that appear in the unformatted file. This appendix can be referred to for information regarding the contents of fields in the unformatted text file, but does not reflect the exact contents of the formatted text file.

Viewing, Retrieving and Archiving Conference Information

Viewing the Conference Records

To open the CDR utility:

*   On the *Collaboration Server Menu*, click **Administration > CDR**.
    The *CDR List* pane opens, displaying a list of the conference CDR records stored in the MCU memory.

The following fields are displayed:

Table 17-1 Conference Record Fields

Field	Description
Display Name	The Display Name of the conference and an icon indicating whether or not the CDR record has been retrieved and saved to a formatted text file. The following icons are used: The CDR record has not been saved. The CDR record has been saved.
Start Time	The actual time the conference started.
GMT Start Time	The actual time the conference started according to Greenwich Mean Time (GMT).
Duration	The actual conference duration.
Reserved Start Time	The reserved start time of the conference. If the conference started immediately this is the same as the *Start Time*.
Reserved Duration	The time the conference was scheduled to last. Discrepancy between the scheduled and the actual duration may indicate that the conference duration was prolonged or shortened.

Table 17-1 *Conference Record Fields (Continued)*

Field	Description
Status	The conference status. The following values may be displayed: • **Ongoing Conference** • **Terminated by User** • **Terminated when end time passed** • **Automatically terminated when conference was empty** – The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. • **Conference never became ongoing due to a problem** • **Unknown error** **Note:** If the conference was terminated by an MCU reset, the status **Ongoing Conference** will be displayed.
File Retrieved	Indicates if the conference record was downloaded using any of the file retrieval buttons in the CDR List pane or the API. • **Yes** - when the conference record was retrieved to any file or using the API. • **No** - when the conference record was not retrieved at all. The File Retrieved field is updated whenever the record is downloaded.

Multi-part CDR File display

When the *Multi-Part CDR* is configured on the *Collaboration Server,* an additional column, *Part Index*, is added to the CDR list.

The *Part Index* column displays the *CDR* file's sequence in the CDR file set:

• *CDRs* that are up to 1MB consist of a single file. Each file has a unique *Display Name* and a *Part Index* of **1**.

• Files included in a *Multi-Part CDR* file sets have the same *Display Name*. The first file of the set is numbered **1** with each additional *CDR* file numbered in an ascending numeric sequence.

Refreshing the CDR List

To refresh the CDR list:

- Click the **Refresh** button, or right-click on any record and then select **Refresh**. Updated conference CDR records are retrieved from the MCU memory.

Retrieving and Archiving Conference CDR Records

To retrieve and archive CDR records:

1 To retrieve a single CDR record, right-click the record to retrieve and then select the required format (as detailed in Table 17-2).
   Alternatively, select the record to retrieve, and then click the appropriate button on the toolbar (as detailed in Table 17-2).

   To retrieve multiple CDR records simultaneously, use standard Windows multi-selection methods.

Table 17-2 Conference Information Retrieval Options

Menu Option	Button	Action
Retrieve		Retrieves the conference information as unformatted data into a file whose extension is .cdr.
Retrieve Formatted XML		Retrieves the conference information as formatted text into a file whose extension is .xml. Note: Viewed when logged in as a special support user.
Retrieve Formatted		Retrieves the conference information as formatted text into a file whose extension is .txt.

The *Retrieve* dialog box opens.
The dialog box displays the names of the destination CDR files.

2 Select the destination folder for the CDR files and then click **OK**.

   If the destination file already exists, you will be asked if you want to overwrite the file or specify a new name for the destination file.
   The files are saved to the selected folder.

> CDR files are not included in the backup process and should be backed up manually by saving the CDR files to a destination device.

18

RMX Manager Application

The *RMX Manager* is the Windows version of the *Web Client*. It can be used instead of the *Web Client* for routine *Collaboration Server* management and for *Collaboration Server* management via a modem connection.For more information on using the *RMX Manager* via a modem connection, see "*Configuring Direct Connections to the Collaboration Server"* on page **F-1**.

Using the *RMX Manager* application, a single user can control a single or multiple MCU units as well as conferences from multiple MCUs. The Polycom RMX 1800 system can be managed and controlled by the RMX Manager application.

The *RMX Manager* can list and monitor:
*   Up to 20 *Collaboration Server* systems in the MCUs pane
*   Up to 800 conferences in the Conferences pane
*   Up to 1600 participants in the Participants pane

The *RMX Manager* is faster than the *Web Client* and can give added efficiency to *Collaboration Server* management tasks, especially when deployed on workstations affected by:
*   Lack of performance due to bandwidth constraints within the LAN/WAN environment.
*   Slow operation and disconnections that can be caused by the anti-phishing component of various antivirus applications.

> Users with *Auditor* authorization level cannot connect to the *RMX* via the *RMX Manager* application and must use the *Web Client*.

The *RMX Manager* application can be installed in your local workstation or accessed directly on the *RMX* system without installing it in your workstation.

Installing the RMX Manager

The *RMX Manager* application can be downloaded from one of the *RMX* systems installed in your site or from Polycom web site at
 http://www.polycom.com/support.

> **New *RMX* Installation Note**
> The *Collaboration Server Installation and First Entry Configuration* must be completed before installing the *RMX Manager* application. For more details, see the *Polycom RMX 1800 Getting Started Guide*, "*Installing the RMX 1800"* on page **2-3**.
> Once the connection to the *Collaboration Server* unit is established and the *Login* window is displayed, the *RMX Manager* application can be installed.

To install RMX Manager (downloading the application from the *RMX*):

1 Start Internet Explorer and connect to one of the *Collaboration Server* units in your site. It is recommended to connect to the *Collaboration Server* installed with the latest software version.

The *Login* screen is displayed. There is a link to the *RMX Manager Installer* at the top of the right edge of the screen.

Link to RMX Manager Installer

1 Click the **Install RMX Manager** link.

The installer verifies the application's requirements on the workstation.
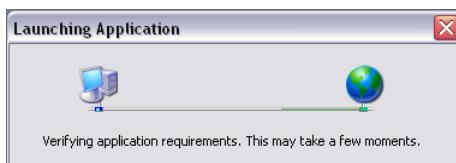
The *Install* dialog box is displayed.

2 Click **Install**.

The installation proceeds.

The installation completes, the application loads and the *RMX Manager - MCUs* screen is displayed.

MCUs Toolbar

MCUs Pane

The first time you start the *RMX Manager* application, the *MCUs* pane is empty.

Starting the RMX Manager Application

Once installed, the *RMX Manager* can be run using the `http://` (non-secured) or `https://` (secured) command in the browser's address line or the Windows *Start* menu.

To use the browser:

1   In the browser's command line, enter:

`http://<MCU Control Unit IP Address>/RMXManager.html`

or

`https://<MCU Control Unit IP Address>/RMXManager.html`

2   Press **Enter**.

To use the Windows Start menu:

1   Click **Start > Programs.**

a   If the *RMX Manager* is displayed in the recently used programs list, click **RMX Manager** in the list to start the application.

or

b   Click **All Programs** > **Polycom** > **RMX Manager**.

The *MCUs* screen is displayed, listing the MCUs currently defined in the *RMX Manager*.
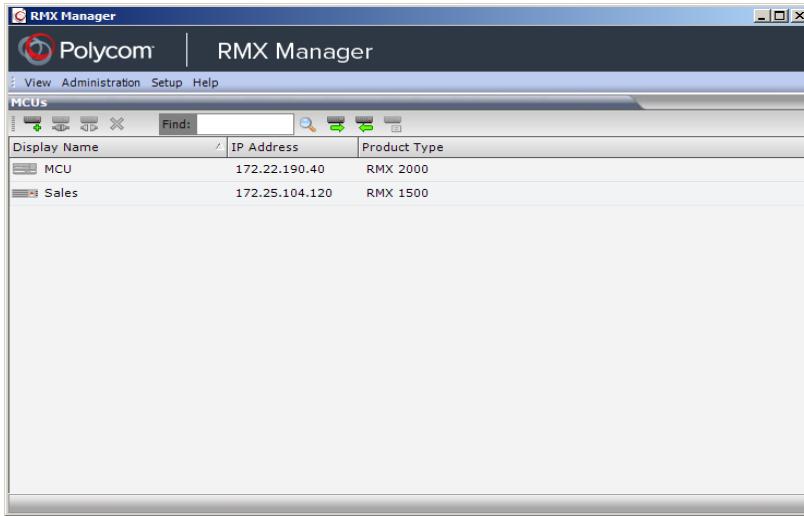
This screen enables you to add additional MCUs or connect to any of the MCUs listed. For details on adding MCUs, see "*Adding MCUs to the MCUs List*" on page **10**.

For each listed MCU, the system displays the following information:

— MCU *Display Name* (as defined in the Add MCU dialog box).

— *IP Address* of the MCU's control unit

— *Product Type* - The MCU type: RealPresence Collaboration Server 800s, RealPresence Collaboration Server (RMX) 1500, RealPresence Collaboration Server (RMX) 2000, or RealPresence Collaboration Server (RMX) 4000.
Before connecting to the MCU for the first time, the *Collaboration Server* type is unknown so "RMX" is displayed instead as a general indication.

To display the *RMX Manager* main screen you must connect to one of the listed *Collaboration Server*s. For more details, see "*Connecting to the MCU*" on page **18-4**.

Connecting to the MCU

Once an MCU is defined, the *RMX Manager* can be connected to it. This allows you to set up conferences, make reservations, monitor On Going Conferences and perform other activities on several MCUs.

> The first *Collaboration Server* unit that is connected to the *RMX Manager* dictates the Authorization Level of Users that can connect to the other MCUs on the list. For example, if the Authorization level of the User POLYCOM is Administrator, all Users connecting to the other MCUs on the list must be Administrators. Each user can have a different login name and password for each of the listed MCUs and they must be defined in the Users list of each of the listed MCUs.

To connect the RMX Manager to an MCU:

1 In the *MCUs* pane or screen, use one of the following methods:

a Double-click the MCU icon.

b Select the *Collaboration Server* to connect and click the **Connect MCU** button.

c   Right-click the MCU icon and then click **Connect MCU**.
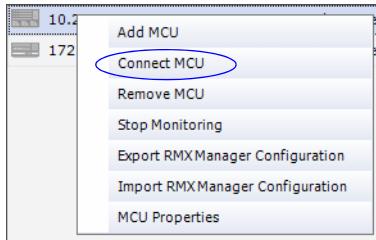
If you are connecting to the MCU from the *MCUs* opening screen and have defined the *Username* and *Password* for the connecting MCU, the system connects to the *Collaboration Server*, and the *RMX Manager Main Screen* is displayed.
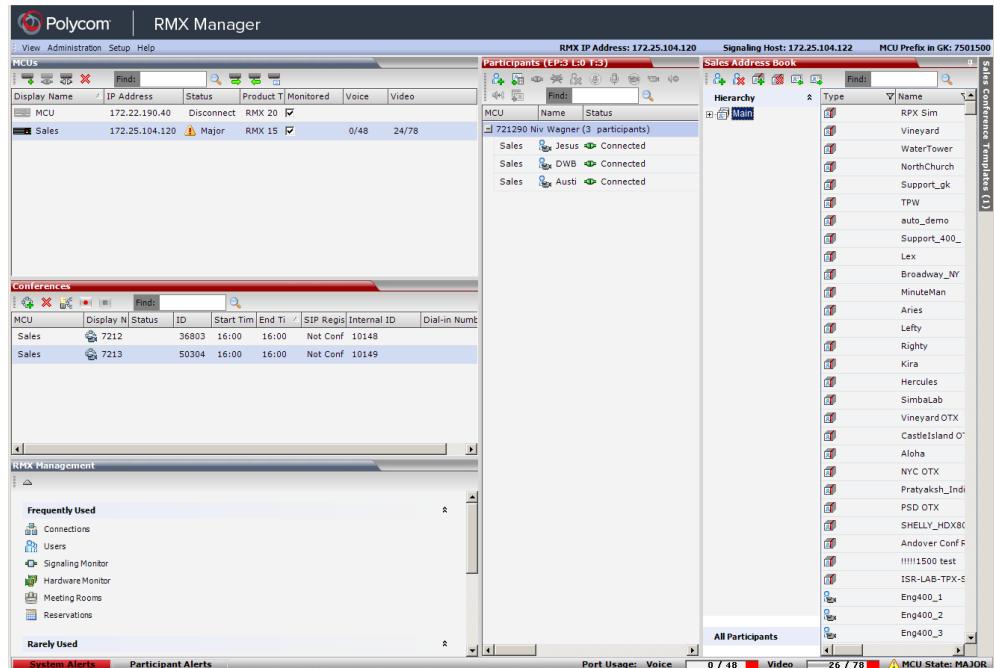
If you are connecting to any MCU from the *MCUs* pane in the *RMX Manager Main Screen* and have defined the *Username* and *Password* for the connecting MCU, the MCU icon changes to connected and its status, type and number of audio and video resources are displayed in the *MCUs* pane.

If the *Username* and *Password* are missing from the MCU parameters, or if the *Remember Me* check box has been cleared, the *Connect* dialog box opens.
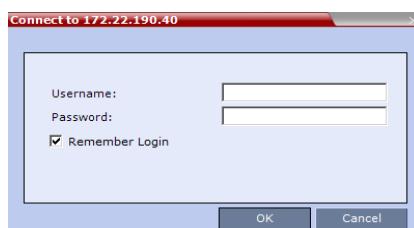
2   In the *Username* field, enter the user name with which you will login to the MCU.

3   In the *Password* field, enter the password as defined for the user name with which you will login to the MCU.

4 To add the user name and password to the MCU properties so you will not have to enter them each time you login to the MCU, make sure that the **Remember Login** check box is selected. Otherwise, clear the **Remember Login** check box.

5 Click **OK**.
The system connects to the *Collaboration Server*, and the *RMX Manager Main Screen* is displayed.

If a User with the entered *Username* and *Password* is not defined in the *Collaboration Server*, an error message is displayed and the system lets you re-enter the *Username* and *Password.*

RMX Manager Main Screen

The *RMX Manager Main Screen* is displayed only when at least one MCU is connected.

This screen is similar to the *Web Client Main Screen* with the addition of the *MCUs* pane. As in the *Web Client*, the panes are displayed according to the *Authorization Level* of the logged in User. The *MCUs* pane is displayed to all users.

Ongoing Conferences Pane

MCUs Pane
The selected MCU is highlighted

List Pane

Address Book Pane

Device Management Pane
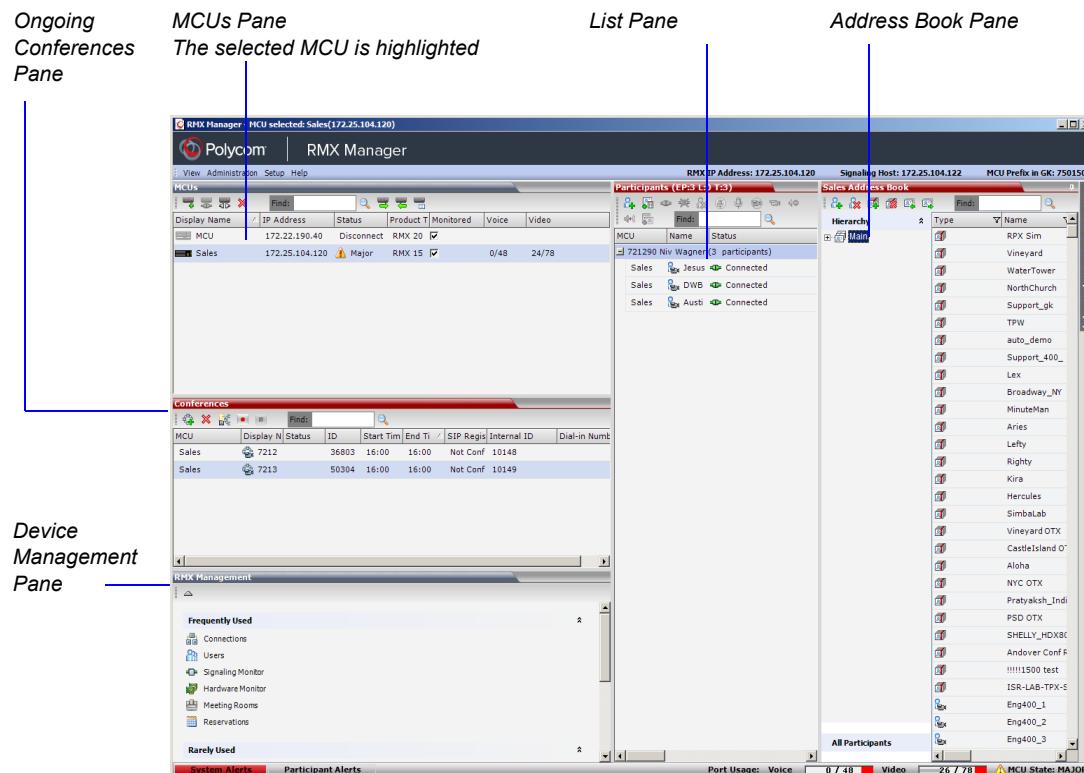
Only one MCU can be selected in the *MCUs* pane. If only one MCU is connected, it is automatically selected. The selected MCU is highlighted.

The menu items, the *Collaboration Server Management* features, the *Address Book* and the *Conference Templates* are all properties of the selected MCU and apply to it.

MCUs Pane

The MCUs pane includes a list of MCUs and a toolbar.
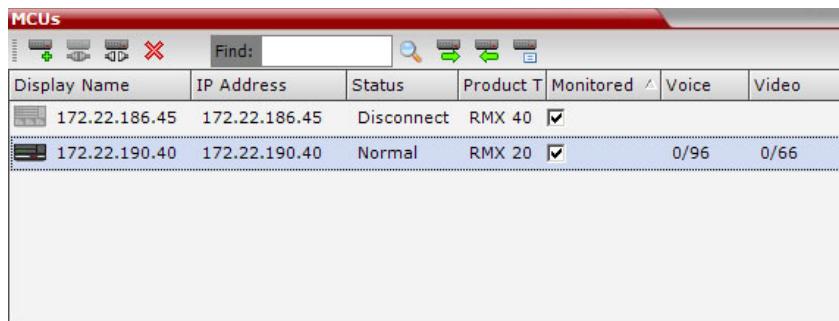
For each listed MCU, the system displays the following information:

- MCU *Display Name* - the name of the MCU and its icon according to its type and connection status. The following icons are available:

Table 18-1 *MCU Icons and Statuses*

Icon	Description
	RealPresence Collaboration Server (RMX) 1500, disconnected.
	RealPresence Collaboration Server (RMX) 1500, connected.
	RealPresence Collaboration Server (RMX) 2000, disconnected.
	RealPresence Collaboration Server (RMX) 2000, connected.
	RealPresence Collaboration Server (RMX) 4000, disconnected.
	RealPresence Collaboration Server (RMX) 4000, connected.
	RealPresence Collaboration Server 1800, disconnected
	RealPresence Collaboration Server 1800, connected
	RealPresence Collaboration Server 800s, disconnected
	RealPresence Collaboration Server 800s, connected

- *IP Address* of the MCU's control unit.
- *Status* - The status of the MCU:
    - *Connected* - the MCU is connected to the *RMX Manager* and can be managed by the *RMX Manager* user.
    - *Disconnected* - The MCU is disconnected from the *RMX Manager*
    - *Major* - The MCU has a major problem. MCU behavior could be affected and attention is required.

- *Product Type* - The MCU type: RMX 1800 , RealPresence Collaboration Server 1500/2000/4000.
  Before connecting to the MCU for the first time, the *Collaboration Server* type is unknown so *Collaboration Server* is displayed instead as a general indication.
- *Monitored* - When checked indicates that the conferences running on this MCU are automatically added to the *Conferences* list and monitored. To stop monitoring the conferences running on this MCU and their participants, clear the *Monitored* check box.
- *Video Resources* - The number of video resources that are available for conferencing.
- *Audio Resource*s - The number of audio resources that are available for conferencing.

MCUs Toolbar

The *MCUs* toolbar contains the following buttons:
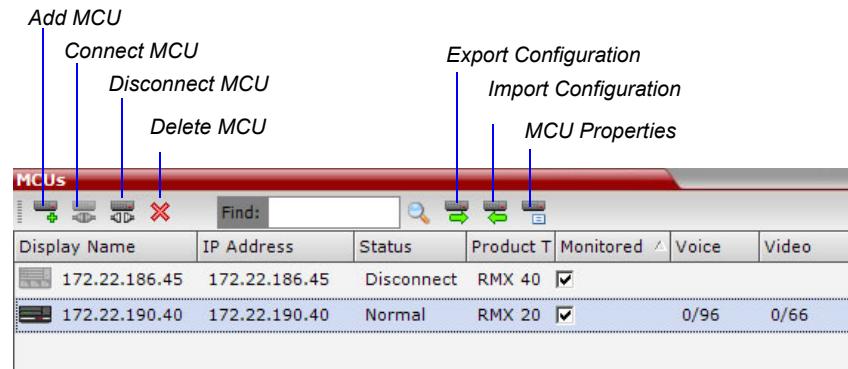
Conferences Pane

The *Conferences* pane lists all the ongoing conferences from all the MCUs that are connected and monitored along with their *MCU*, *Status*, *Conference ID*, *Start Time* and *End Time* data. The number of ongoing conferences is displayed in the pane's title.

The *Conferences* list toolbar contains the following buttons:

Monitoring conferences

New conferences run on MCUs selected for *Monitoring* are automatically added to the *Conferences* list. You can sort the conferences by MCU by clicking the **MCU** column heading in the *Conferences* table. Conferences run on MCUs that are connected but not monitored are not listed.

Using Windows multiple selection methods to select conferences, participants from several conferences running on different MCUs can be listed in the *Participants* list pane.

Starting a new conference

When starting a new conference, you must first select the MCU to run the conference in the MCUs pane.

Collaboration Server Management

The *Collaboration Server Management* pane lists the entities **of the selected MCU** that need to be configured to enable the *Collaboration Server* to run conferences. Only users with Administrators permission can modify these parameters.

The *Collaboration Server Management* pane is divided into two sections:

- **Frequently Used** – parameters often configured monitored or modified.

- **Rarely Used** – parameters configured during initial system set-up and rarely modified afterward.

List Pane

The *List* pane displays details of the participants connected to the conferences selected in the *Conferences* pane or the item selected in *Collaboration Server Management* pane. The title of the pane changes according to the selected item.

When selecting an item in the *Collaboration Server Management* pane it applies only to the MCU selected in the MCUs list. In such a case, the system displays the name of the selected MCU in the List pane title.

Status Bar

The *Status Bar* at the bottom of the *RMX Web Client* contains *System* and *Participant Alerts* tabs as well as *Port Usage Gauges* and an *MCU State* indicator.
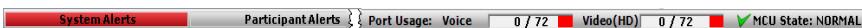
System Alerts

Lists system problems of all connected MCUs (even if the MCU is not monitored). The alert indicator flashes red when at least one system alert is active. The flashing continues until a user with Operator or Administrator permission reviews the list.

The *System Alerts* can be sorted by MCU by clicking the *MCU* header in the *System Alerts* table.

The *System Alerts* pane is opened and closed by clicking the **System Alerts** button in the left corner of the *Status Bar*.

Active Alarms

Faults List

For more information about **Active Alarms** and **Faults List,** see "*System and Participant Alerts" on page* **19-1**.

Participant Alerts

Lists the participants of all monitored MCUs that are experiencing connection problems. The list is sorted by MCU and conference.

The *Participant Alerts* can be sorted by MCU by clicking the *MCU* header in the *Participant Alerts* table.

The *Participant Alerts* pane is opened and closed by clicking the **Participant Alerts** button in the left corner of the *Status Bar*.

Port Usage Gauges

The *Port Usage* gauges display for the selected MCU:

- The total number of *Video* ports in the system according.
- The number of *Video* ports in use.
- The *High Port Usage* threshold.

For more details, see the *Polycom RMX 1800 Getting Started Guide*, *"Port Usage Gauges"* on page **3-7**.

MCU State

The *MCU State* indicator displays the status of the selected MCU.

For more details, see the *Polycom RMX 1800 Getting Started Guide*, *"MCU State"* on page **3-7**.

Address Book

Displays the *Address Book* of the **selected** MCU (regardless of its *Monitored* status). The *Address Book* is a list of *Participants* and *Groups* that have been defined on the **selected** *Collaboration Server*.

The information in the *Address Book* can be modified only by an administrator. All *Collaboration Server* users can, however, view and use the *Address Book* to assign participants to conferences.

The name of the selected *Collaboration Server* is displayed in the title of the Address Book pane. For more details, see the *Polycom RMX 1800 Getting Started Guide*, *"Address Book"* on page **3-8**.

Conference Templates

Conference Templates enable administrators and operators to create, save, schedule and activate identical conferences.

The *Conference Templates* pane lists the Conference Templates that have been defined on the **selected** *Collaboration Server* (regardless of its *Monitored* status).

The *Conference Templates* pane is initially displayed as a closed tab. The name of the selected *Collaboration Server* and the number of saved *Conference Templates* is indicated on the tab.

For more details, see the *Polycom RMX 1800 Getting Started Guide*, *"Conference Templates"* on page **3-9**.

Adding MCUs to the MCUs List

The *RMX Manager* can connect to one or several *Collaboration Server*s simultaneously. If the site's configuration includes more than one MCU, or when a new MCU is added to your configuration, and you want to monitor and control all MCUs from within the same window, you must add the MCU to the MCUs list.

> The *Collaboration Server* must be installed and its IP addresses properly configured in the Management Network Service before defining its connection parameters in the *RMX Manager* application.

To add the MCU to the list of MCUs being managed, define the MCU's connection parameters.

To add a *Collaboration Server* unit:

1 On the *MCUs* toolbar, click the **Add MCU** ⊞ button to add an MCU to the MCU list. The *Add MCU* dialog box opens.

2 Define the following parameters:
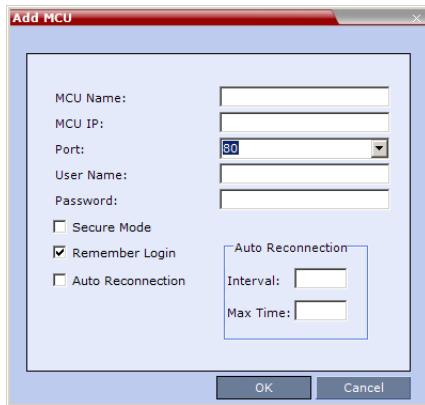
Table 19   *MCU Properties*

Field	Description
MCU Name	Enter the name of the MCU on the network.
MCU IP	Enter the IP address of the MCU's Control Unit. The IP address must be identical to the one configured in the MCU during first entry Configuration. For more details, see the *Polycom RMX 1800 Getting Started Guide*, "*Procedure 1: First-time Power-up*" on page **2-8**.
Port	Enter the number of the port used for communication and data transactions between the *Collaboration Server* unit and the *RMX Manager*. For standard connection, enter **80**. For a Secured connection (using TLS or SSL), enter **443**.
Username	Enter the user name with which you will login to the MCU. A User with this name must be defined in the *Collaboration Server* Users list. The system is shipped with a default User whose name is POLYCOM.
Password	Enter the password as defined for the user name with which you will login to the MCU. The system is shipped with a default User whose password is POLYCOM.
Secure Mode	**Optional**. Select this check box to connect to the *Collaboration Server* with SSL and work in Secure Mode.
Remember Login	This check box is automatically selected, and it enables the usage of the user name and password entered in this dialog box when connecting to the *Collaboration Server*. If this check box is cleared, the user is prompted for the user name and password when connecting to this *Collaboration Server* unit.
Auto Reconnection	Select this check box to automatically reconnect to the *Collaboration Server* if the connection between the *RMX Manager* and the MCU is broken.

Field	Description
Interval	Enter time in seconds between reconnect ion attempts to the *Collaboration Server*. For example, if you enter 10, the system will wait 10 seconds between the connection attempts.
Max Time	Enter the maximum amount of time in seconds that the *Collaboration Server* is allowed to try to reconnect. If the *Collaboration Server* reconnects before the allotted time frame the count down timer is halted. For example, if you enter 100, the system will stop trying to reconnect if it has failed to do so within 100 seconds.

3   Click **OK**.
The MCU is added to the MCUs pane.

4   If required, repeat steps 1-3 to define additional *Collaboration Server* units.

The *MCUs* pane contains the list of all defined MCUs.
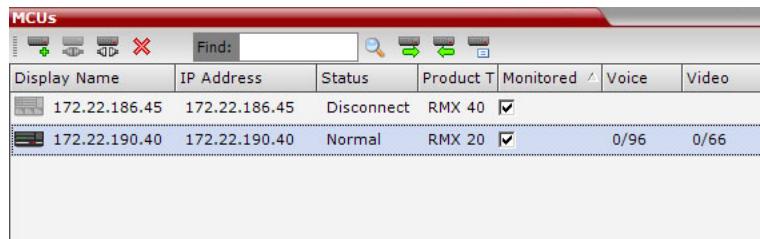
Starting a Conference

There are several ways to start a conference:

- Clicking the *New Conference* button in the *Conferences* pane. For more information, see "*Starting a Conference from the Conferences Pane*" on page **13**.
- Dialing in to a Meeting Room defined on any of the MCUs.
  - A Meeting Room is a conference that is saved on the MCU. It remains in passive mode until it is activated by the first participant, or the meeting organizer dialing in. For more information about Meeting Rooms, see "*Meeting Rooms*" on page **6-1**.
- Dialing in to an Ad Hoc Entry Queue defined on one of the MCUs which is used as the access point to the MCU.

  For a detailed description of Ad Hoc Entry Queues, see "*Entry Queues*" on page **7-1**.
- Start a *Reservation:*
  - If the *Start Time* of the *Reservation* is past due the conference becomes ongoing immediately.
  - If the *Start Time* of the *Reservation* is in the future the conference becomes ongoing, at the specified time on the specified date.

  For more information, see "*Starting a Reservation*" on page **18-13**.
- Start any *Conference Template* saved in the *Conference Templates* list.
  For more information, see "*Starting an Ongoing Conference or Reservation From a Template*" on page **18-14**.

Starting a Conference from the Conferences Pane

To start a conference from the Conference pane:

1   In the *MCUs* pane, select the MCU to run the conference.

2   In the *Conferences* pane, click the **New Conference** (🌐) button.

The *New Conference – General* dialog box opens.
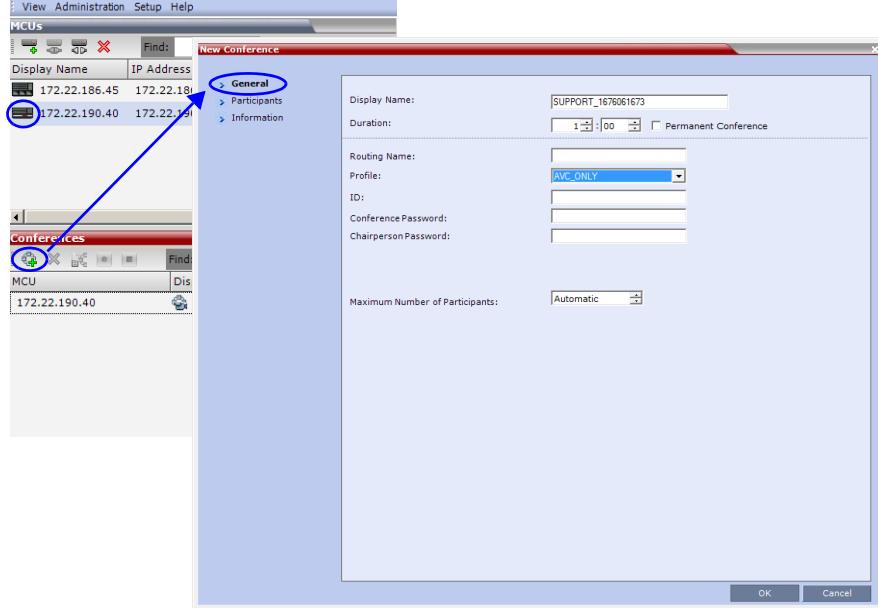
The system displays the conference's default *Name*, *Duration* and the default *Profile*, which contains the conference parameters and media settings.

The *Collaboration Server* automatically allocates the conference *ID*, when the conference starts.

In most cases, the default conference *ID* can be used and you can just click **OK** to launch the conference. If required, you can enter a conference *ID* before clicking **OK** to launch the conference.

If you are the meeting chairperson or organizer using the *RMX Web Client* to start your own meeting, you need to communicate the default conference ID (or the one you created) to the other conference participants so they can dial in.

You can use the *New Conference - General* dialog box to modify the conference parameters. If no defined participants are to be added to the conference, or you do not want to add additional information, click **OK**.

For more details, see the *Polycom RMX 1800 Getting Started Guide*, *"Starting a Conference from the Conferences Pane"* on page **3-12**.

Starting a Reservation

To start a conference from the Reservation Calendar:

1   In the *MCUs* pane, select the MCU to run the conference.

2   In the *Collaboration Server Management* pane, click the *Reservation Calendar* button (📅).

The *Reservation Calendar* is displayed.

Name of selected MCU
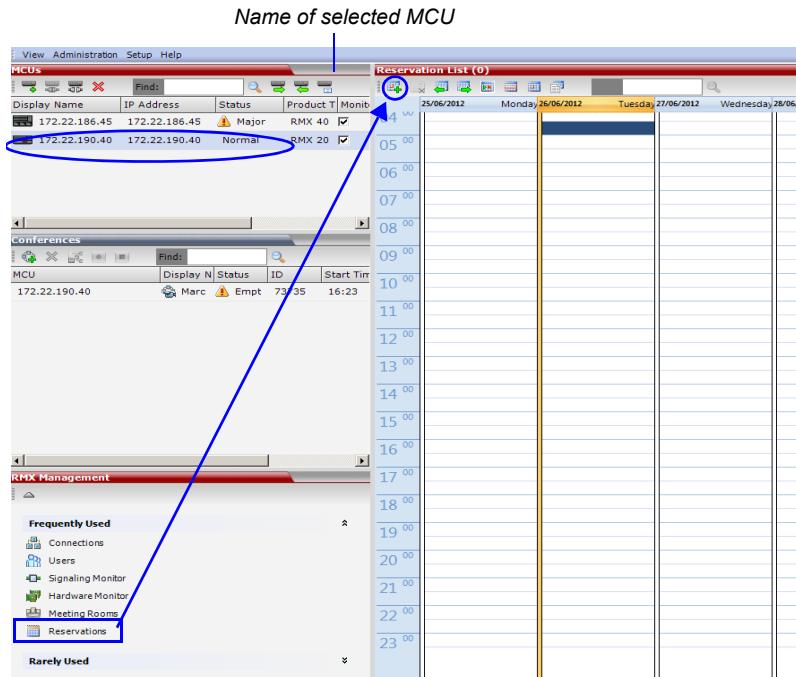
3 Click the **New Reservation** ( ) button.

For more information, see the *Polycom RMX 1800 Getting Started Guide*, "*Starting a Reservation"* on page **3-20**.

Starting an Ongoing Conference or Reservation From a Template

An ongoing conference or a Reservation can be started from any Conference Template saved in the *Conference Templates* list of the selected MCU.

To start an ongoing conference or a reservation from a Template:

1 In the *MCUs* pane, select the MCU to run the conference.

1 In the *Conference Templates* list, select the Template you want to start as an ongoing conference.

2 Click the **Start Conference from Template** ( ) button to start a conference or

Schedule Reservation from Template ( ) button to schedule a reservation.
or
Right-click and select **Start Conference from Template** to start an ongoing conference or **Schedule Reservation from Template** to schedule a reservation.

Name of selected MCU   Name of selected MCU
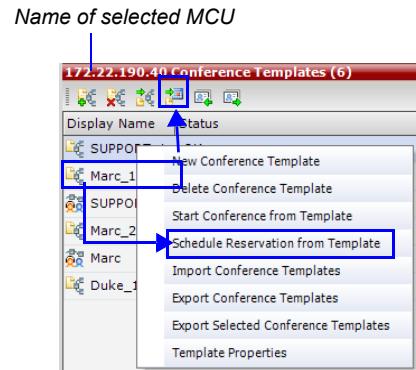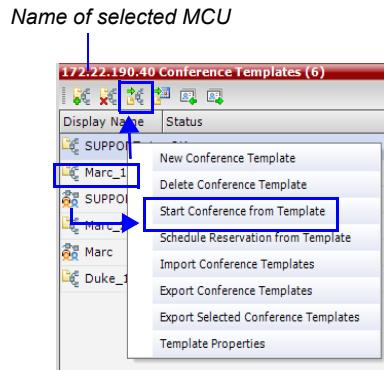
The conference is started.

For detailed description of *Conference Templates*, see "*Using Conference Templates*" on page **11-2**.

Monitoring Conferences

When MCUs are connected to the *RMX Manager* they are automatically monitored, that is, any ongoing conference that is started on that MCU is automatically added to the Conferences pane and its participants are monitored.

To list participants from several conferences (running on the same or different MCUs):

>> In the *Conferences* pane, using Windows multiple selection methods, select the conferences whose participants you want to list.

The participants are displayed in the *Participants* list pane.

By default, the participants are grouped by conferences, and the name of the MCU is displayed in the first column of the properties table, enabling sorting according to MCU name.

Grouping the Participants by MCU

The Participants can be grouped by MCU and then by conferences.

To change the display mode for the Participants pane:

>> On the *Collaboration Server Menu*, click **View > Group by MCU**.
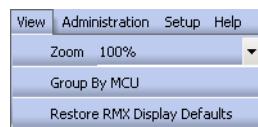
The *Participants* pane display changes accordingly.

To toggle between the two display modes, click **View > Group by MCU.**

Start Monitoring/Stop Monitoring

By default, all conferences running on connected *Collaboration Server*s are monitored.

You can stop the automatic monitoring of conferences on a specific MCU in one of the following methods:

- By clearing the check box in the *Monitored* column in the *MCUs* pane.
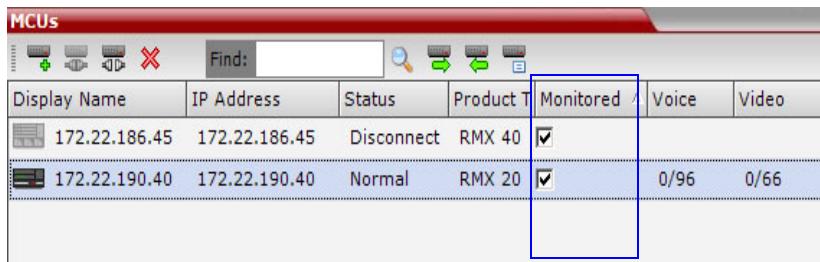
- Right-clicking the MCU icon and selecting **Stop Monitoring**.

The check box is cleared in the Monitored column.

To start monitoring again, click the check box in the *Monitored* column in the *MCUs* pane, or right-clicking the MCU icon and selecting **Start Monitoring**.

Modifying the MCU Properties

You can view the currently defined MCU settings, and modify them when required, for example, change the MCU name, IP address or Secured mode.

Use this procedure to add the *Username* and *Password* to the properties of the MCU that was automatically added to the MCU list when installing the *RMX Manager*. This enables automatic login when connecting the MCU to the *RMX Manager*.

You can modify the MCU properties when the MCU is connected or disconnected.

To view and/or modify the MCU Properties:

1 Use one of the following methods:

   a Select the MCU to disconnect and click the **MCU Properties** button.

b   Right-click the MCU icon and then click **MCU Properties**.

```
Add MCU
Disconnect MCU
Remove MCU
Stop Monitoring
Export RMX Manager Configuration
Import RMX Manager Configuration
MCU Properties
```
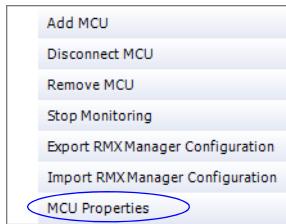
The *MCU Properties* dialog box opens.

2   Define/modify the required parameters. For details, see "*MCU Properties*" on page **11**.

3   Click **OK**.

Disconnecting an MCU

An MCU can be disconnected from the *RMX Manager*, without removing it from the *MCUs* list.

To disconnect an MCU:

1   Use one of the following methods:

a   Select the MCU to disconnect and click the **Disconnect MCU** button.

b   Right-click the MCU icon and then click **Disconnect MCU**.

```
Add MCU
Disconnect MCU
Remove MCU
Stop Monitoring
Export RMX Manager Co
```
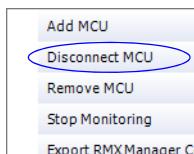
The MCU icon changes to disconnected and any ongoing conference running on that MCU will not be monitored in this *RMX Manager*; they are removed from the *Conferences* pane. This MCU can still be monitored and controlled by other users.

Removing an MCU from the MCUs Pane

An MCU can be removed from the *RMX Manager*. This function should be used if the MCU hardware was disconnected and removed from the network.

To Remove an MCU from the list:

1   Use one of the following methods:

a   Select the MCU to disconnect and click the **Delete** button.

b   Right-click the MCU icon and then click **Remove MCU**.

```
Add MCU
Disconnect MCU
Remove MCU
Stop Monitoring
Export RMX Manager Co
```
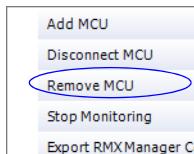
A confirmation message is displayed.

2 Click **OK** to confirm or **Cancel** to abort the operation.

The MCU icon is removed from the MCUs pane.

Changing the RMX Manager Language

You can change the language of the *RMX Manager* menus and dialog boxes. Only one language can be selected at a time and the *RMX Manager* application must be restarted after changing the display language.

To select a language:

1 On the *RMX Manager* menu, click **Setup > Customize Display Settings > Multilingual Settings**.

The *Multilingual Settings* dialog box opens, displaying the current language selection.
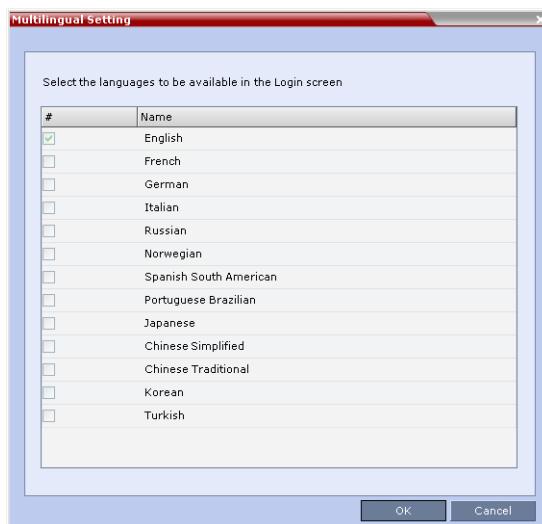
2 Click the check box of the required language. Only one language can be selected.

3 Click **OK**.

4 Restart the *RMX Manager* application to implement the language change.

Import/Export RMX Manager Configuration

The *RMX Manager* configuration that includes the MCU list and the multilingual selection can be save to any workstation/PC on the network and imported to any *Multi-RMX Manager* installed in the network. This enables the creation of the MCUs list once and distributing it to all *RMX Manager* installations on the network.

In addition, when upgrading to a previous version, the MCU list is deleted, and can be imported after upgrade.

The exported file is save in XML format and can be edited in any text editor that can open XML files.

To Export the RMX Manager Configuration:

1   In the *Multi-RMX Manager*, click the **Export RMX Manager Configuration** button in the toolbar, or right-click anywhere in the MCUs pane and then click **Export RMX Manager Configuration**.
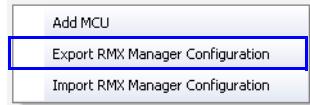
The *Export RMX Manager Configuration* dialog box opens.

2   Click the **Browse** button to select the location of the save file, or enter the required path in the *Export Path* box.
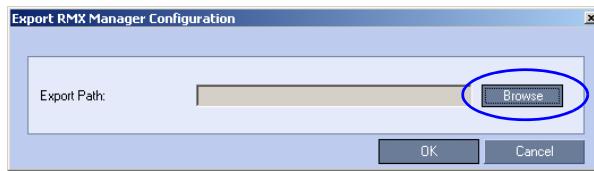
The selected file path is displayed in the *Export Path* box.

3   Click **OK** to export the *RMX Manager* configuration.

To Import the RMX Manager Configuration:

1   In the *Multi-RMX Manager*, click the **Import RMX Manager Configuration** button in the toolbar, or right-click anywhere in the MCUs pane and then click **Import RMX Manager Configuration**.
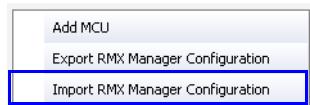
The *Import RMX Manager Configuration* dialog box opens.
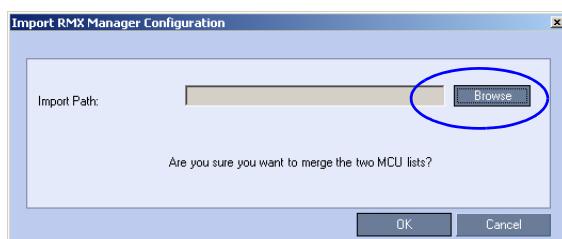
2 Click the **Browse** button to select the saved file, or enter the required path in the *Export Path* box.

The *Open* dialog box is displayed.
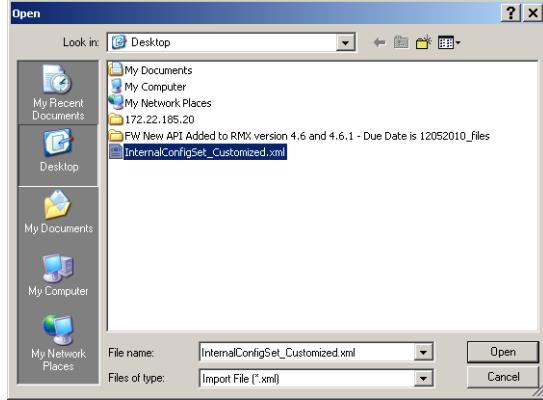
3 Select the XML file previously saved, and click the **Open** button.

The selected file path is displayed in the *Import Path* box.

4 Click OK to import the file.

5

19
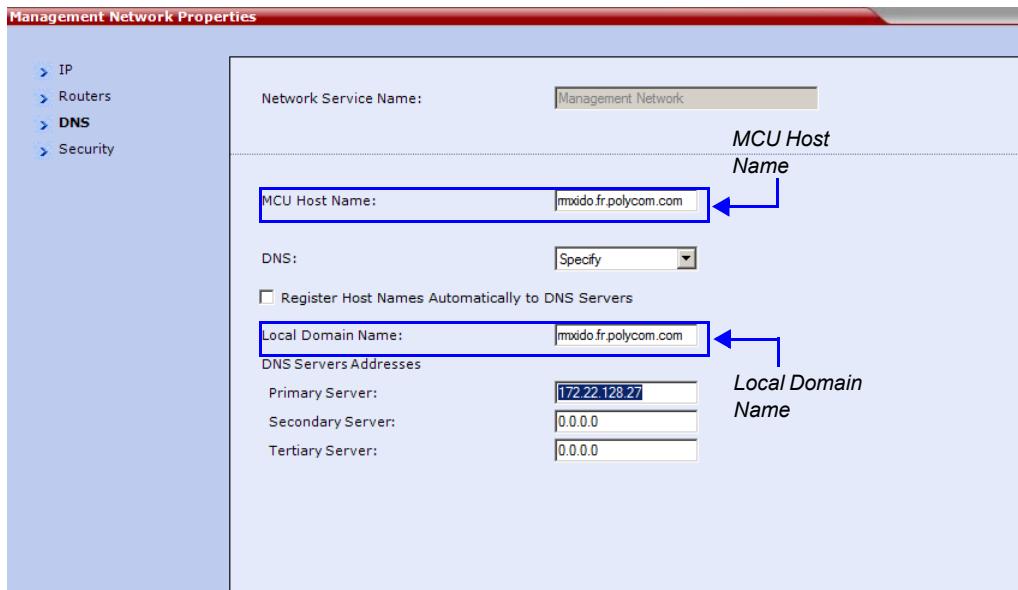
Collaboration Server Administration and Utilities

System and Participant Alerts

The MCU alerts users to any faults or errors the MCU encountered during operation. Two indication bars labeled System Alerts and Participant Alerts signal users of system errors by blinking red in the event of an alert.

System Alerts
indication bar

Participant Alerts
indication bar
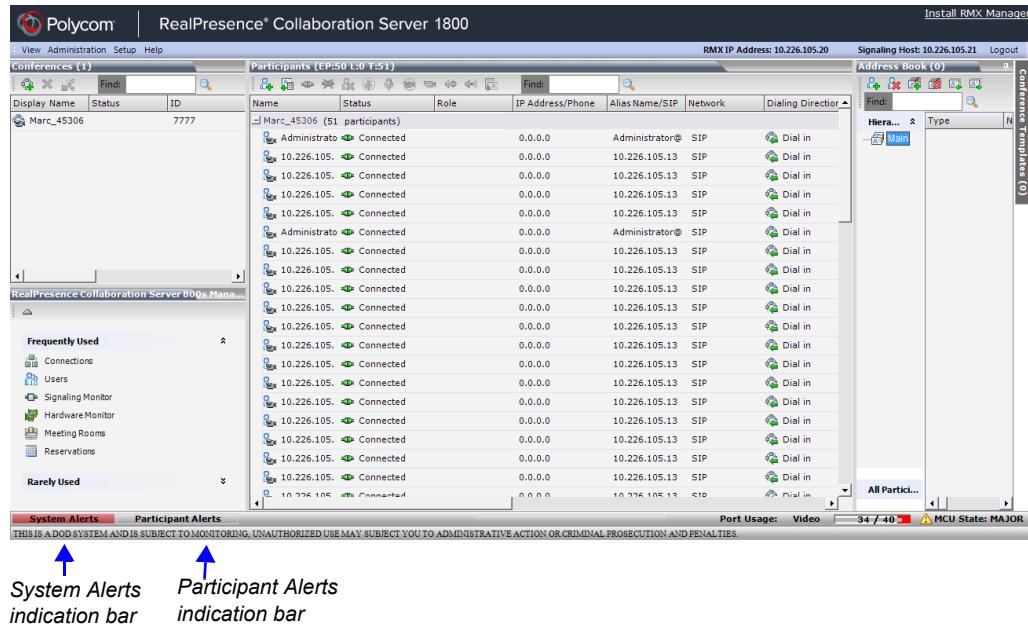
The *System Alerts* indication bar blinks red prompting the user to view the active alarms. Once viewed, the *System Alerts* indication bar becomes statically red until the errors have been resolved in the MCU.

The *Participants Alerts* indication bar blinks red indicating participant connection difficulties in conferences. Once viewed, the *Participant Alerts* indication bar becomes statically red until the errors have been resolved in the MCU.

System Alerts

System Alerts are activated when the system encounters errors such as a general or card error. The system errors are recorded by the *Collaboration Server* and can be generated into a report that can be saved in *.txt format.

To view the System Alerts list:

1 Click the red blinking **System Alerts** indication bar.

The *Active Alarms* pane opens. This screen indicates what events have not been resolved.

The following columns appear in the *Active Alarms* pane:

Table 19-1 Active Alarms Pane Columns

Field	Description
ID	An identifying number assigned to the system alert.
Time	Lists the local date and time that the error occurred. This column also includes the icon indicating the error level (as listed in the level column).
GMT Time	Lists the date and time according to Greenwich Mean Time (GMT) that the error occurred.
Category	Lists the type of error. The following categories may be listed: • **File** – indicates a problem in one of the files stored on the MCU's hard disk. • **Card** – indicates problems with a card. • **Exception** – indicates software errors. • **General** – indicates a general error. • **Assert** – indicates internal software errors that are reported by the software program.
Category (cont.)	• **Startup** – indicates errors that occurred during system startup. • **Unit** – indicates problems with a unit.
Level	Indicates the severity of the problem, or the type of event. There are three fault level indicators: 🛑 – Major Error ❗ – System Message ⌛ – Startup Event
Code	Indicates the problem, as indicated by the error category.
Process Name	Lists the type of functional process involved.
Description	When applicable, displays a more detailed explanation of the cause of the problem.

For more information about the Active Alarms, see *Appendix B: "Active Alarms"* on page **B-1**.

2 Click one of the following two buttons to view its report in the *System Alerts* pane:

	Active Alarms (default) – this is the default reports list that is displayed when clicking the System Alerts indication bar. It displays the current system errors and is a quick indicator of the MCU status.
	Faults Full List - A list of all system faults. Note: Viewed when logged in as a special support user.
	Faults List – a list of faults that occurred previously (whether they were solved or not) for support or debugging purposes.

3 To save the *Active Alarms, Faults Full List* or *Faults* report:

— to a text file, click the **Save to Text** button

— to an XML file, click the **Save to XML** button

The **Save to XML** button is only available when logged in as a special support user.

The *Save* dialog window opens.

4 Select a destination folder and enter the file name.

5 Click **Save**.

Participant Alerts

Participant Alerts enables users, participants and conferences to be prompted and currently connected. This includes all participants that are disconnected, idle, on standby or waiting for dial-in. Alerts are intended for users or administrators to quickly see all participants that need their attention.

To view the Participants Alerts list:

1 Click the red blinking **Participants Alerts** indication bar.

The *Participant Alerts* pane opens.

The *Participant Alerts* pane displays similar properties to that of the *Participant List* pane. For more information, see the *Polycom RMX 1800 Getting Started Guide,* "*Participant Level Monitoring"* on page **3-36**.

2 To resolve participant issues that created the *Participant Alerts*, the administrator can either **Connect** , **Disconnect** or **Delete** a participant.

RMX Time

To ensure accurate conference scheduling, the MCU has an internal clock that can function in standalone mode, or in synchronization with up to three *Network Time Protocol* (*NTP*) servers.

Guidelines

- *NTP Version 4* is the only supported protocol.
- If applicable, daylight saving adjustments must be implemented by the administrator whether the MCU is in standalone mode or synchronized with *NTP Servers*.

Altering the clock

The MCU's date and time can be set manually or enabled to synchronize with external *NTP* servers.

To Alter the MCU Time:

1 On the *Collaboration Server* menu, click **Setup > RMX Time** to open the *RMX Time* dialog box.
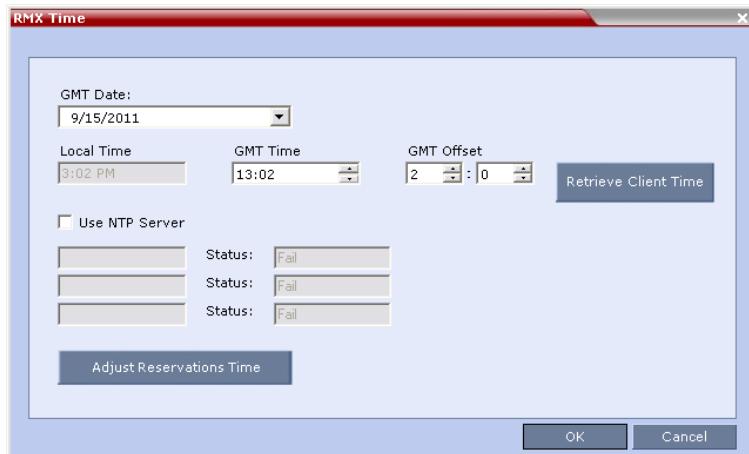
2 View or modify the following fields:

Table 19-2 *RMX Time – Fields Properties*

Field	Description
GMT Date	The date at Greenwich, UK.
Local Time	The MCU's local time settings, are calculated from the *GMT Time* and the *GMT Offset*.
GMT Time	The MCU's current *GMT Time* settings. Select the *Up* or *Down* arrows to alter the *GMT Time* on the MCU.

Table 19-2 RMX Time – Fields Properties (Continued)

Field	Description
GMT Offset	The time zone difference between Greenwich and the MCU's physical location in hours and minutes. Select the *Up* or *Down* arrows to alter the *GMT Offset* time on the MCU. To enter a negative offset either type a minus in the hour box or use the down arrow and decrease the offset below zero.
Retrieve Client Time	Click this button to automatically update the MCU's *GMT Date, Time* and *Offset* to match that of the workstation.
Use NTP Server	Select this check box to synchronize the time with up to three *NTP* servers. When selected, the manual *GMT Date* and *GMT Time* setting options are disabled. The *GMT Offset* fields are still active. To implement this mode an external connection to an *NTP* server must be enabled. Enter the IP addresses of the required *NTP* servers in order of precedence. The *Status* field indicates whether registration with the *NTP Server* failed or succeeded. Note: The*Collaboration Server* will not use a time source such as a Windows-based, W32Time service (SNTP) time service. Only full-featured (below Stratum 16) NTP Servers are considered sufficiently reliable for high-accuracy timing environments.
Adjust Reservations Time (*Button*)	Use this button to adjust the start time of all the reservations in one operation. For more information see "*Adjusting the Start Times of all Reservations"* on page **9-16**

After resetting the MCU a delay may occur when synchronizing with the external NTP server.

Resource Management

Resource Capacity

The following table lists the resource capacity in various *RealPresence Collaboration Server (RMX) 1500/2000/4000* configurations.

Table 20

Resource Type/Video Resolution	3 Video Acceleration Cards	2 Video Acceleration Cards	1 Video Acceleration Card
Audio-only	100	100	100
H.261 CIF p25/30	50	35	15

Table 20

Resource Type/Video Resolution	3 Video Acceleration Cards	2 Video Acceleration Cards	1 Video Acceleration Card
H.263 CIF p25/30	100	70	35
H.264 CIF p25/30	100	70	35
H.264 CIF p50/60	100	70	35
H.263 4CIF p25/30	100	70	35
H.264 4CIF p25/30	100	70	35
H.264 4CIF p50/60	100	70	35
H.264 720p 25/30	100	70	35
H.264 720p 50/60	50	35	17
H.264 1080p 25/30	50	35	17
H.264 1080p 50/60	25	17	8

Resource Usage

From Version 8.1, *only the MPMx Media Card* and *Card Configuration Mode* are supported.

From Version 8.1, *Fixed Resource Capacity Mode* is not supported. Only the *Flexible Resource Capacity Mode* is supported.

AVC Conferencing - Continuous Presence

Video resources usage varies according to the video resolution used by the endpoints. The higher the video resolution (quality), the greater the amount of video resources consumed by the MCU. Table 19-3 shows the number of video resources used for each resolution.

Forcing Video Resource Allocation to CIF Resolution

From Version 8.1, *Fixed Resource Capacity Mode* is not supported. Only the *Flexible Resource Capacity Mode* is supported.

From *Version 8.1 MPM+* media cards are not supported.

From Version 8.1, *Fixed Resource Capacity Mode* is not supported. Only the *Flexible Resource Capacity Mode* is supported.

You can set the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters. This forcing saves resources and enables more endpoints to connect to conferences.

The forcing is done by modifying the system configuration and it applies to all conferences running on the MCU.

You can specify the endpoint types for which resource allocation can be forced to CIF resource, enabling other types of endpoints to use higher resolutions in the same conference. For example, you can force the system to allocate one CIF video resource to CMAD and VSX endpoints while HDX endpoints can connect using SD or HD video resources.

Once the endpoint connects to the conference, its type is identified by the Collaboration Server and, if applicable, the Collaboration Server will connect it using one CIF resource, even if a higher resolution can be used.

To force CIF resource:

1   On the Collaboration Server menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2   In the *MCMS_PARAMETERS* tab, click the **New Flag** button.

The *New Flag* dialog box is displayed.

3   In the *New Flag* field enter the flag name: **FORCE_CIF_PORT_ALLOCATION**

4   In the *Value* field enter the product type to which the CIF resource should be allocated. Possible values are:

— **CMA Desktop** for CMA desktop client

— **VSX nnnn** where nnnn represents the model number for example, VSX 8000.

You can define several endpoint types, listing them one after the other separated by semicolon (;).
For example, CMA Desktop;VSX 8000.

5   Click **OK**.
The new flag is added to the flags list.

Reset the MCU for changes to take effect. For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1800 Administrator's Guide, "Resetting the Collaboration Server (RMX)"* on page **19-54**.

To cancel the forcing of CIF resource:

1   On the Collaboration Server menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2   In the *MCMS_PARAMETERS* tab, double-click or select the flag **FORCE_CIF_PORT_ALLOCATION** and click the **Edit Flag** button.

3   In the *New Value* field, clear the value entries.

4   Click **OK**.

Reset the MCU for changes to take effect. For more details, see the *RMX Administrator's Guide*, "" on page **19-54**

Resource Report

When viewing the Collaboration Server resource report, the resource allocations are described in AVC HD units.

The *Resource Report* displays the real time resource usage. The *Resource Report* includes a graphic representation of the resource usage. One resource report is available for all resource usage.

Displaying the Resource Report

1   In the main toolbar, click **Administration > Resource Report**.
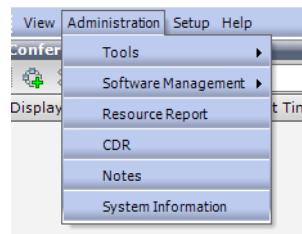
For each resource type, the Resource Report includes the following columns:

Table 19-4 *Resource Report Fields Parameters*

Column	Description
Type	The type of audio/video resources available.
Occupied	The number of MCU resources that are used by connected AVC participants or reserved for defined participants.
Free	The number of MCU resources available for connecting AVC endpoints.
Total	The *Total* column displays the total number of resources of that type (*Occupied* and *Free*).

•

The actual number of occupied or free resources can also be displayed by moving the cursor over the columns of the bar graph. Moving the cursor over the *Video* bar displays the following:

8 Occupied Video Resources

64 Free Video Resources
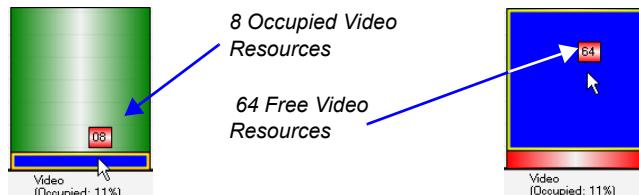
When viewing the Collaboration Server resource report for mixed CP and SVC conferences, the resource allocations are described in AVC HD720p30 units. A port ratio of 1 AVC HD port will equal 2 AVC SD ports, which equals 3 SVC ports (in a non-mixed conference).

When the Collaboration Server is reporting the available capacity, it will appropriately round up the remaining capacity to the nearest whole value of available ports. For example, one SVC endpoint in a conference is equal to *1/3* of the resource value. The resource report displays this as one full resource used. Two SVC endpoints is equal to *2/3* of the resource value. Therefore, the resource report displays this as one full resource used, and so forth.

The following table explains the actual resource capacity utilization for both CP only and mixed CP and SVC conferences:

Table 19-5   Resource Capacity Allocation Per Port Type

Port Type	Non-Mixed Conferences	Mixed CP and SVC Conferences
AVC HD	1	1.5 *
AVC SD	0.5	0.75 *
AVC CIF	0.333	0.75 *
SVC	0.333	0.333

* Resources are consumed at this rate only **after** the conference contains mixed endpoints.

Table 19-6   Resource Capacity Utilization Per Port Type per MPMx Card

Port Type	Maximum Ports in Non-mixed Conferences	Maximum Ports in Mixed CP and SVC Conferences
Maximum number of licences	30	
AVC HD	30	20
AVC SD	60	40
AVC CIF	90	40
SVC	90	90

The Resource Capacity Utilization table indicates the total amount of ports used for each port type for one MPMx media board in full capacity.

The following diagram displays the RealPresence Collaboration Server (RMX) Resource Report, displaying a resource graph that indicates the number of voice and video ports that are available or occupied in the MCU.
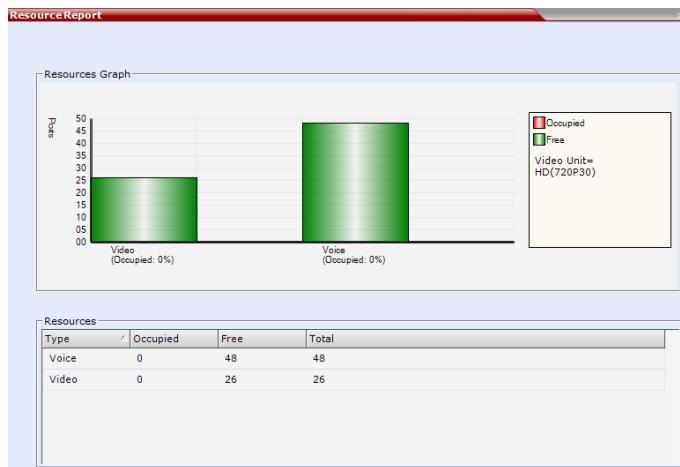
Port Usage Threshold

The *Collaboration Server* can be set to alert the administrator to potential port capacity shortages. A capacity usage threshold can be set as a percentage of the total number of licensed ports in the system.

When the threshold is exceeded, a *System Alert* is generated.

The default port capacity usage threshold is 80%.

The administrator can monitor the MCU's port capacity usage via the *Port Gauge* in the *Status Bar* of the *Collaboration Server Web Client*.

Setting the Port Usage Threshold

To Set the Port Usage Threshold:

1 In the *Setup* menu, click **Port Gauge** to open the *Port Gauge* dialog box.
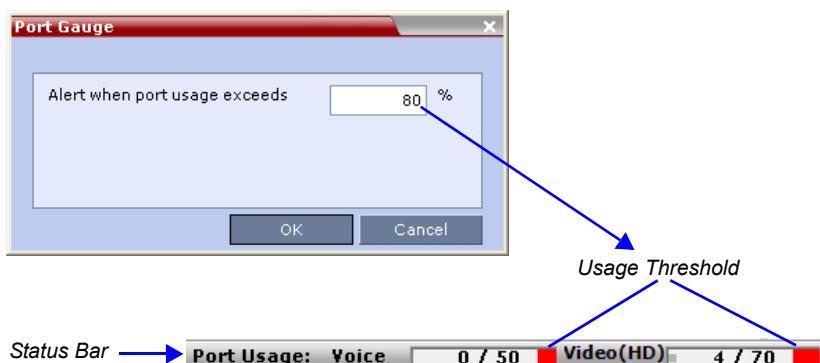
Enter the value for the percentage capacity usage threshold.
The value is applied to the Audio and video resources .The high Port Usage threshold represents a percentage of the total number of video or voice ports available. It is set to

indicate when resource usage is approaching its maximum, resulting in no free resources to run additional conferences. When port usage reaches or exceeds the threshold, the red area of the gauge flashes. The default port usage threshold is 80%.

2 Click **OK.**

SIP Dial-in Busy Notification

When the system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default), it enables the MCU to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the MCU whose audio resource usage exceeded the Port Usage threshold.

The *Collaboration Server* will send a SIP busy response to SIP audio endpoints when:

• The system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default)

• The port usage threshold for Audio resources is exceeded. The threshold is defined in the **Setup > Port Gauge** dialog box.
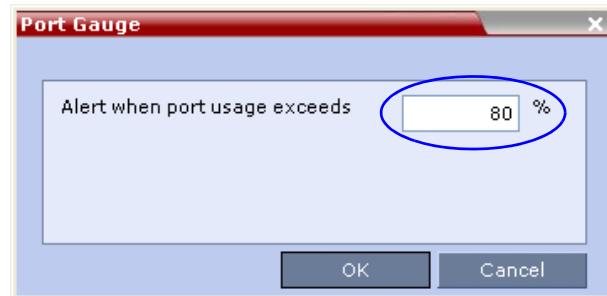
When the flag is set to YES, the system will allow SIP audio endpoints to connect to the MCU until the Port Usage threshold is reached. Once this threshold is exceeded, the SIP audio endpoints will not be able to connect, ensuring that the remaining system resources can be used by all other connections, including SIP video, and H.323 cascaded links. When the call is rejected by the MCU because of lack of resources, the appropriate indication will be sent by the MCU to the SIP audio endpoint.

For example, if the *Port Gauge* threshold is set to 80%, when 80% of the **Audio resources** are used, the system will not allow additional SIP audio endpoints to connect and will send a busy notification to the endpoint.

This does not affect the video resources usage.

Port Usage Gauge

The *Port Usage Gauges* are displayed in the *Status Bar* at the bottom of the *Collaboration Server Web Client* screen.

Status Bar   Port Usage Gauge
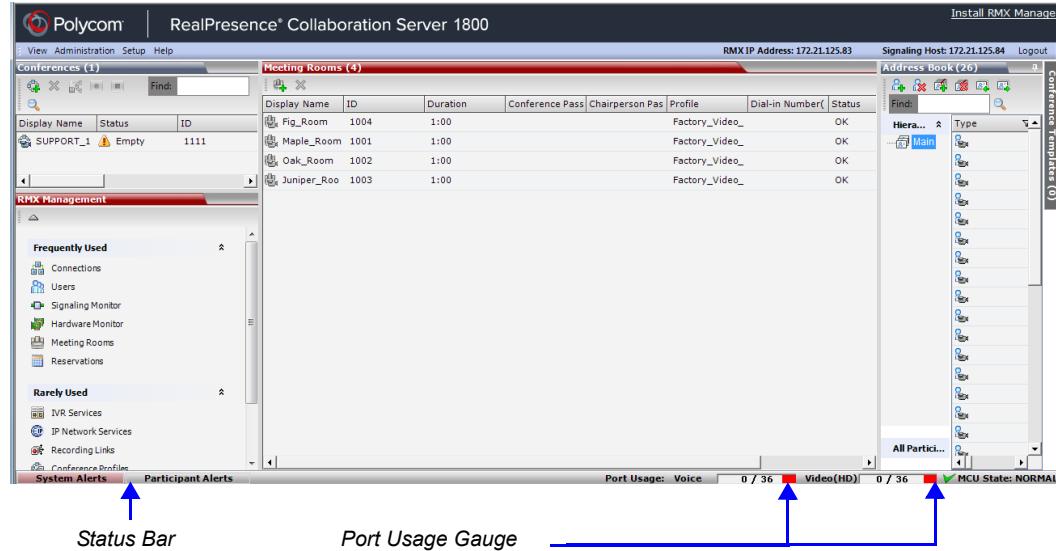
The *Port Usage* gauges indicate:

* The total number of *Video* or *Voice* ports in the system
* The number of *Video* and *Voice* ports in use.
* The *High Port Usage* threshold.

Total Allocated Video Ports In System
Video Ports In Use
Video Port Usage Indicator

Total Allocated Audio Ports In System
Audio Ports In Use
Audio Port Usage Indicator

Audio and Video Port Usage Threshold
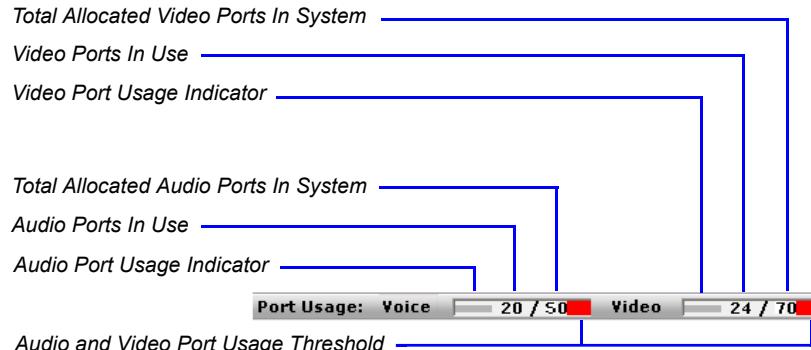
The basic unit used for reporting resource usage in the Port Gauges is HD720p30. Results are rounded to the nearest integer.

System Information

System Information includes *License Information* and general system information.

To view the System Information properties box:

>> On the Polycom RMX 1800 menu, click **Administration > System Information**.

The *System Information* properties box is displayed.
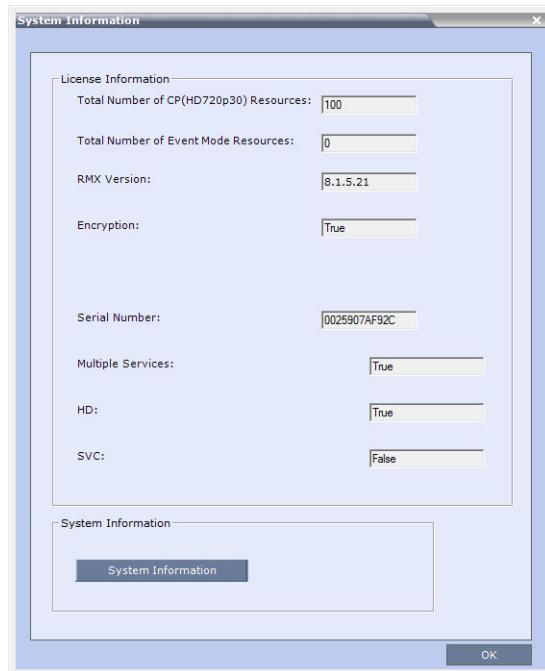
The *System Information* properties box displays the following information:

Table 19-7 System Information

Field	Description
Total Number of CP(HD720p30) Resources	Displays the number of HD720p30 video participants licensed for the system. Each HD720p30 resource represents one 3 CIF video resources.
Total Number of Event Mode Resources	Displays the number of video/voice participants licensed for a system in Event Mode Licensing. It also determines the conference type that is available on the system. 0 - indicates that this Licensing mode is disabled for this system.
RMX Version	Displays the *System Software Version* of the RMX™.
Encryption	Indicates whether *Encryption* is included in the MCU license. Encryption is not available in all countries. Range: True / False
Serial Number	Displays the *Serial Number* of the Collaboration Server unit.
Multiple Services	A *Multiple Services* license is installed.

Table 19-7 *System Information (Continued)*

Field	Description
HD	Indicates if the MCU is licensed to connect endpoints at *HD* resolutions in *Continuous Presence* conferences.
Polycom Partners	Indicates that the *System Software* contains features for the support of specific *Polycom Partner* environments.

SNMP (Simple Network Management Protocol)

SNMP enables managing and monitoring of the MCU status by **external** managing systems, such as HP OpenView or through web applications.

The Collaboration Server's implementation of SNMPv3 is FIPS 140 compliant.

MIBs (Management Information Base)

MIBs are a collection of definitions, which define the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each of the definitions written in the MIB.

The SNMP systems poll the MCU according to the MIB definitions.

Traps

The MCU is able to send Traps to different managers. Traps are messages that are sent by the MCU to the SNMP Manager when an event such as MCU Reset occurs.

Guidelines

• *Version 1, Version 2* and *Version 3* traps are supported.
• When *SNMPv3* is selected only *SNMPv3 Queries* and *Traps* receive responses.
• A mixture of *Version 1, Version 2* and *Version 3* traps is not permitted.

MIB Files

The H.341 standard defines the MIBs that H.320 and H.323 MCUs must comply with. In addition, other MIBs should also be supported, such as MIB-II and the ENTITY MIB, which are common to all network entities.

The MIBs are contained in files in the *SNMP MIBS* sub-directory of the Collaboration Server root directory. The files should be loaded to the SNMP external system and compiled within that application. Only then can the SNMP external application perform the required monitoring tasks.

> The MULTI-MEDIA_MIB_TC must be compiled before compiling the other MIBs.

Private MIBs

• *RMX-MIB (RMX-MIB.MIB)*
  — Contains the statuses of the Collaboration Server: Startup, Normal and Major.
  — Contains all the Alarms of the Collaboration Server that are sent to the SNMP Manager.

Support for MIB-II Sections

The following table details the MIB-II sections that are supported:

Table 19-8   Supported MIB-II Sections

Section	Object Identifier
system	mib-2 1
interfaces	mib-2 2
ip	mib-2 4

The Alarm-MIB

MIB used to send alarms. When a trap is sent, the Alarm-MIB is used to send it.

H.341-MIB (H.341 – H.323)

*   Gives the address of the gatekeeper.
*   Supports H.341-MIB of SNMP events of H.323.

Standard MIBs

This section describes the MIBs that are included with the Collaboration Server. These MIBs define the various parameters that can be monitored, and their acceptable values.

Table 19-9   Standard MIBs

MIB Name	Description
MULTI-MEDIA-MIB-TC (MULTIMTC.MIB)	Defines a set of textual conventions used within the set of Multi Media MIB modules.
H.320ENTITY-MIB (H320-ENT.MIB)	This is a collection of common objects, which can be used in an H.320 terminal, an H.320 MCU and an H.320/H.323 gateway. These objects are arranged in three groups: Capability, Call Status, and H.221 Statistics.
H.320MCU-MIB (H320-MCU.MIB)	Used to identify managed objects for an H.320 MCU. It consists of four groups: System, Conference, Terminal, and Controls. The *Conference* group consists of the active conferences. The *Terminal* group is used to describe terminals in active MCU conferences. The *Controls* group enables remote management of the MCU.
H323MC-MIB (H323-MC.MIB)	Used to identify objects defined for an H.323 Multipoint Controller. It consists of six groups: System, Configuration, Conference, Statistics, Controls and Notifications. The *Conference* group is used to identify the active conferences in the MCU. The *Notifications* group allows an MCU, if enabled, to inform a remote management client of its operational status. **Note:** The Collaboration Server supports only one field in H.341-H323MC MIB. The Collaboration Server reports the Gatekeeper address using H.341-H323MC MIB – 323McConfigGatekeeperAddress (0.0.8.341.1.1.4.2.1.1.4) in response to a query from a manager.

Table 19-9   Standard MIBs

MIB Name	Description
MP-MIB (H323-MP.MIB)	Used to identify objects defined for an H.323 Multipoint Processor, and consists of two groups: Configuration and Conference. The *Configuration* group is used to identify audio/video mix configuration counts. The *Conference* group describes the audio and video multi-processing operation.
MIB-II/RFC1213-MIB (RFC1213.MIB)	Holds basic network information and statistics about the following protocols: TCP, UDP, IP, ICMP and SNMP. In addition, it holds a table of interfaces that the Agent has. MIB-II also contains basic identification information for the system, such as, Product Name, Description, Location and Contact Person.
ENTITY-MIB (ENTITY.MIB)	Describes the unit physically: Number of slots, type of board in each slot, and number of ports in each slot.

Unified MIB

The Collaboration Server uses the Polycom Unified MIB, in addition to the RMX specific MIB. The Polycom Unified MIB is an MIB that is used by many Polycom products. The following table describes the information provided by the Collaboration Server in the Unified MIB.

Table 19-10 Unified MIB SNMP Fields

Name	Type	Description
Debug	Boolean	Indicates whether the unit is in a debugging state.
IncomingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to receive incoming H.323 calls.
OutgoingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to make outgoing H.323 calls.
HDBitrateThrshld	Integer	The minimum bit rate required by endpoints in order to connect to an HD conference.
MaxCPRstln	Integer	Maximum resolution of a CP conference.
MaxCPRstlnCfg	Integer	Configured resolution for a CP conference.
EndpointDispayName	String	The name of the MCU that is displayed on the screen of endpoints that are connecting to the conference.
PALNTSC	NTSC/PAL/AUTO	The video encoding of the RMX.
SeparateMgmtNet	Boolean	Indicates whether management network separation is enabled.
NumPorts	Integer	Total number of ports.
NumVideoPorts	Integer	Number of ports configured for video.

Table 19-10 Unified MIB SNMP Fields (Continued)

Name	Type	Description
ServiceH323	Integer	Indicates the status of H.323 capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
ServiceSIP	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
ServiceISDN	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
RsrcAllocMode	Fixed/ Flexible	The resource allocation method which determines how the system resources are allocated to the connecting endpoints.
McuSystemStatus	Integer	System State.
FanStatus	Boolean	Status of the hardware fan.
PowerSupplyStatus	Boolean	Status of the power supply.
IntegratedBoardsStatus	Boolean	Status of the integrated boards.
UltraSecureMode	Boolean	Indicates whether the RMX is operating in Ultra Secure Mode.
ChassisTemp	Integer	The temperature of the chasis.
NumPortsUsed	Integer	Number of ports currently in use.
NewCallsPerMinute	Integer	New calls in the last minute.
ScsfNewCallsPerMinute	Integer	Successful new calls in the last minute.
FldNewCallsPerMinute	Integer	Failed new calls in the last minute.
PctScsflNewCalls	Integer	Percentage of new calls in the last minute which were successful.
CallsEndedScsflPerMin	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailedPerMin	Integer	Number of calls in the last minute which ended with a failure code.
CallsEndedScsfl	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailed	Integer	Number of calls in the last minute which ended with a failure code.
NumActvCnfrncs	Integer	Number of active conferences.

Traps

Three types of traps are sent as follows:

1 ColdStart trap. This is a standard trap which is sent when the MCU is reset.

```
coldStart notification received from: 172.22.189.154 at 5/20/
  2007 7:03:12 PM

  Time stamp: 0 days 00h:00m:00s.00th

  Agent address: 172.22.189.154 Port: 32774 Transport: IP/UDP
  Protocol: SNMPv2c Notification

  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP

  Community: public

  Enterprise: enterprises.8072.3.2.10

  Bindings (3)

    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:00m:00s.00th

    Binding #2: snmpTrapOID.0 *** (oid) coldStart
```

Figure 1   *An Example of a ColdStart Trap*

2 Authentication failure trap. This is a standard trap which is sent when an unauthorized community tries to enter.

```
authentication Failure notification received from:
  172.22.189.154 at 5/20/2007 7:33:38 PM

  Time stamp: 0 days 00h:30m:27s.64th

  Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
  Protocol: SNMPv2c Notification

  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP

  Community: public

  Enterprise: enterprises.8072.3.2.10

  Bindings (3)

    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:30m:27s.64th

    Binding #2: snmpTrapOID.0 *** (oid) authenticationFailure
```

Figure 2   *An Example of an Authentication Failure Trap*

3 Alarm Fault trap. The third trap type is a family of traps defined in the POLYCOM-RMX-MIB file, these traps are associated with the Collaboration Server active alarm and clearance (proprietary SNMP trap).

```
rmxFailedConfigUserListInLinuxAlarmFault notification received
  from: 172.22.189.154 at 5/20/2007 7:04:22 PM
 Time stamp: 0 days 00h:01m:11s.71th
 Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
 Protocol: SNMPv2c Notification
 Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
 Community: public
 Bindings (6)
   Binding #1: sysUpTime.0 *** (timeticks) 0 days
   00h:01m:11s.71th
   Binding #2: snmpTrapOID.0 *** (oid)
   rmxFailedConfigUserListInLinuxAlarmFault
   Binding #3: rmxAlarmDescription *** (octets) Insufficient
   resources
   Binding #4: rmxActiveAlarmDateAndTime *** (octets) 2007-6-
   19,16:7:15.0,0:0
   Binding #5: rmxActiveAlarmIndex *** (gauge32) 2
   Binding #6: rmxActiveAlarmListName *** (octets) Active
   Alarm Table
 *   Binding #7: rmxActiveAlarmRmxStatus *** (rmxStatus) major
```

Figure 3   *An Example of an Alarm Fault Trap*

Each trap is sent with a time stamp, the agent address, and the manager address.

Status Trap

The MCU sends status traps for the status **MAJOR** - a trap is sent when the card/MCU status is MAJOR.

All traps are considered "MAJOR".

RMX MIB entities that do not generate traps.

The following table lists the entities that appear in the RMX MIB of the SNMP that do not generate traps. These traps will be displayed as Faults in the System Alerts pane (at the bottom of the Collaboration Server (RMX) Web Client screen.

Table 19-11 SNMP MIB entities that do not generate traps

Key	Description	Comment
5002	Resource process did not receive the Meeting Room list during startup.	
5004	Task terminated	
5008	Low Processing Memory	
5009	Low system Memory	
5010	High system CPU usage	
5014	High CPU utilization	

Table 19-11 *SNMP MIB entities that do not generate traps (Continued)*

Key	Description	Comment
5016	Process idle	
5107	Failed to open Apache server configuration file	
5108	Failed to save Apache server configuration file	
5110	A private version is loaded	
5111	NTP synchronization failure	
5112	Invalid date and time	
5116	Incorrect Ethernet Settings	
5117	Smart Report found errors on hard disk	
5118	Invalid MCU Version	
5150	Music file error	
5205	Unspecified problem	
5207	Unit not responding	
5209	Failed to mount Card folder	
5401	The Log file system is disabled	
5450	Action redirection failure	
5601	Process terminated	
5602	Terminal initiated MCU reset	
5603	User initiated MCU reset	
5604	Internal MCU reset	
5605	MCU reset	
5606	MCU Reset to enable Diagnostics mode	
5607	Startup process failure	
5801	Polycom default User exists. For security reasons, it is recommended to delete this User and create your own User.	Only in non-Ultra Secure Mode
5904	Single clock source	
5950	MCU is not configured for AVF gatekeeper mode	
5652	Hard disk error /AA_HARD_DISK_FAILURE	Not in use
5551	Port configuration modified	Not in use
5011	Used for testing the Active Alarms mechanism	Not in use

Table 19-11 SNMP MIB entities that do not generate traps (Continued)

Key	Description	Comment
5001	License not found	Not in use (Product activation failure is trapped)

Defining the SNMP Parameters in the Collaboration Server

The SNMP option is enabled via the *Collaboration Server Web Client* application.

The addresses of the Managers monitoring the MCU and other security information are defined in the *Collaboration Server Web Client* application and are saved on the MCU's hard disk. Only users defined as Administrator can define or modify the SNMP security parameters in the *Collaboration Server Web Client* application.

To enable SNMP option:

1 In the *Collaboration Server Web Client* menu bar, click **Setup > SNMP**.

The *Collaboration Server-SNMP Properties - Agent* dialog box is displayed.
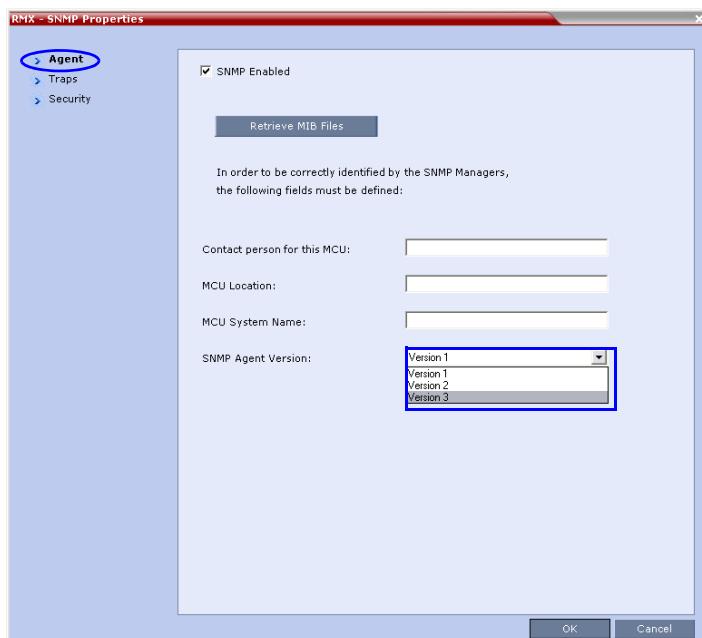
This dialog box is used to define the basic information for this MCU that will be used by the SNMP system to identify it.

2 In the *Agent* dialog box, click the **SNMP Enabled** check box.

3 Click the **Retrieve MIB Files** button to obtain a file that lists the MIBs that define the properties of the object being managed.

The *Retrieve MIB Files* dialog box is displayed.

4 Click the **Browse** button and navigate to the desired directory to save the MIB files.

5   Click **OK**.
The path of the selected directory is displayed in the *Retrieve MIB Files* dialog box.

6   Click the **Save** button.
The MIB files are saved to the selected directory.

7   Click **Close** to exit the *Retrieve MIB Files* dialog box.

8   In the *Agent* dialog box, define the parameters that allow the SNMP Management System and its user to easily identify the MCU.

Table 19-12 Collaboration Server-SNMP Properties - Agent Options

Field	Description
Contact person for this MCU	Type the name of the person to be contacted in the event of problems with the MCU.
MCU Location	Type the location of the MCU (address or any description).
MCU System Name	Type the MCU's system name.

9   Click the **Traps** tab.
The *Collaboration Server-SNMP Properties – Traps* dialog box opens.
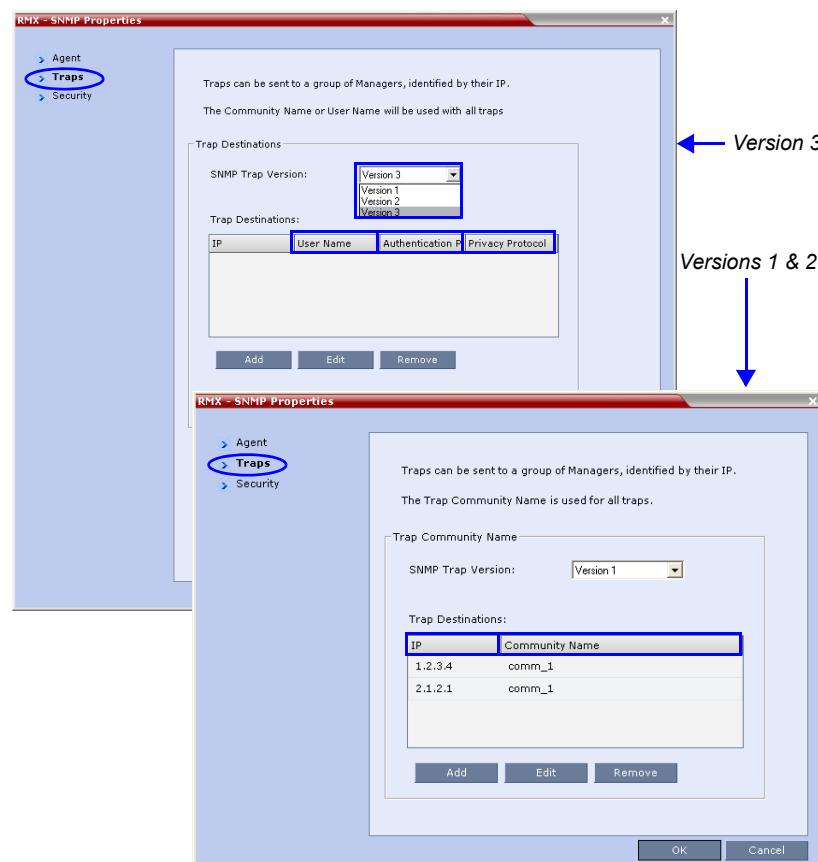
Traps are messages sent by the MCU to the SNMP Managers when events such as MCU Startup or Shutdown occur. Traps may be sent to several SNMP Managers whose IP addresses are specified in the *Trap Destinations* box.

10 Define the following parameters:

Table 19-13 SNMPv3 - Traps

Field	Description		
SNMP Trap Version	Specifies the version, either Version 1 2 or 3 of the traps being sent to the IP Host. Polycom software supports the standard SNMP version 1 and 2 traps, which are taken from RFC 1215, convention for defining traps for use with SNMP. **Note:** The SNMP Trap Version parameters must be defined identically in the external SNMP application.		
Trap Destination	This box lists the currently defined IP addresses of the Manager terminals to which the message (trap) is sent.		
	IP	Enter the IP address of the SNMP trap recipient.	All Versions
	Community Name	Enter the Community Name of the manager terminal used to monitor the MCU activity	Version 1 and Version 2
	User Name	Enter the name of the user who is to have access to the trap.	Version 3
	Authentication Protocol	Enter the authentication protocol: MD5 or SHA.	
	Privacy Protocol	Enter the privacy protocol: DES or AES.	
	Engine ID	Enter an Engine ID to be used for both the Agent and the Trap. Default: Empty	

11 Click the **Add** button to add a new Manager terminal.

Depending on the *SNMP Trap Version* selected, one of the two following *New Trap Destination* dialog boxes opens.
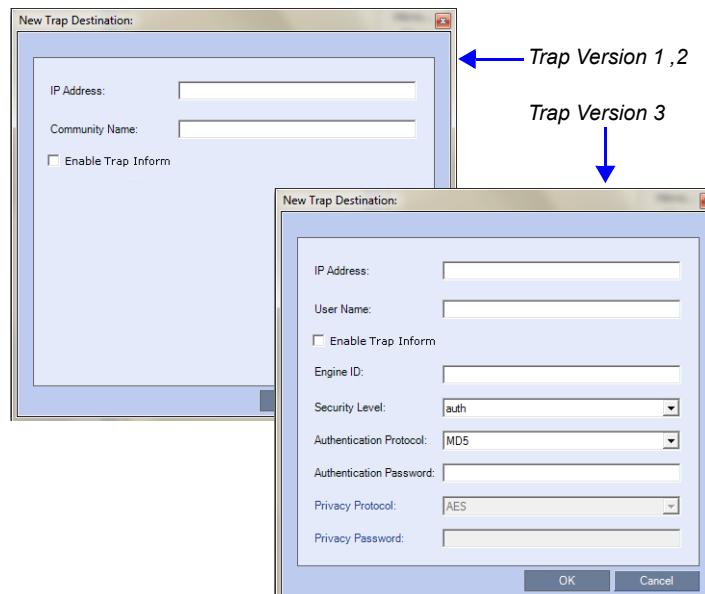
12 Define the following parameters:

Table 19-14 SNMPv3 - Traps

Field	Description	Version
IP Address	Enter the IP address of the SNMP trap recipient.	
Enable Trap Inform	An Inform is a *Trap* that requires receipt confirmation from the entity receiving the *Trap*. If the *Engine ID* field (*Version 3*) is empty when *Enable Trap Inform* has been selected, the *Engine ID* is set by the *Client*.	1,2,3
Community Name	Enter the Community Name of the manager terminal used to monitor the MCU activity	1, 2

Table 19-14 *SNMPv3 - Traps (Continued)*

Field	Description	Version
User Name	Enter the name of the user who is to have access to the trap.	
Engine ID	Enter an *Engine ID* to be used for the *Trap*. This field is enabled when the *Enable Trap Inform* check box is selected. If the *Enable Trap Inform* check box is cleared the *Engine ID* of the *Agent* is used. The *Engine ID* is comprised of up to 64 Hexadecimal characters. Default: Empty	
Security Level	Select a *Security Level* from the drop-down menu. **Range:** *No Auth, No Priv; Auth, No Priv; Auth, Priv* **Default:** Auth, Priv	
Authentication Protocol	Enter the authentication protocol: MD5 or SHA. The availability of the MD5 Authentication Protocol as a selectable option is controlled by adding the SNMP_FIPS_MODE System Flag to system.cfg and setting its value. A value of YES means that MD5 will neither be displayed as selectable option nor supported. Range: YES/NO. Default: NO.	3
Authentication Password		
Privacy Protocol	Enter the privacy protocol: DES or AES. The availability of the DES Privacy Protocol as a selectable option is controlled by adding the SNMP_FIPS_MODE System Flag to system.cfg and setting its value. A value of YES means that DES will neither be displayed as a selectable option nor supported. Range: YES/NO. Default: NO.	
Privacy Password		

13 Type the **IP Address** and the **Community name** of the manager terminal used to monitor the MCU activity, and then click **OK**.

The *Community name* is a string of characters that will be added to the message that is sent to the external Manager terminals. This string is used to identify the message source by the external Manager terminal.

The new *IP Address* and *Community name* is added to the *Trap Destinations* box.

a To delete the IP Address of a Manager terminal, select the address that you wish to delete, and then click the **Remove** button.

The IP address in the *Trap Destinations* box is removed.

14 Click the **Security** tab.

The *Collaboration Server-SNMP Properties – Security* dialog box opens.
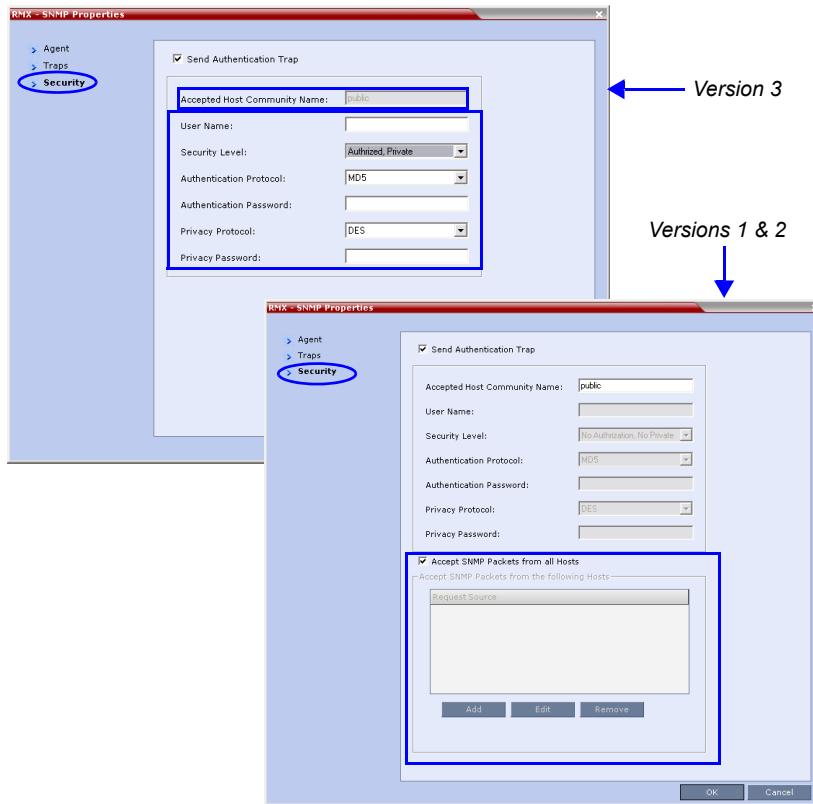
This dialog box is used to define whether the query sent to the MCU is sent from an authorized source. When the "*Accept SNMP packets from all Hosts*" is disabled, a valid query must contain the appropriate community string and must be sent from one of the Manager terminals whose IP address is listed in this dialog box.

15 Define the following parameters:

Table 19-15 SNMP - Security

Field	Description	
Send Authentication Trap	Select this check box to send a message to the SNMP Manager when an unauthorized query is sent to the MCU. When cleared, no indication will be sent to the SNMP Manager.	Versions 1 & 2
Accept Host Community Name	Enter the string added to queries that are sent from the SNMP Manager to indicate that they were sent from an authorized source. **Note:** Queries sent with different strings will be regarded as a violation of security, and, if the Send Authentication Trap check box is selected, an appropriate message will be sent to the SNMP Manager.	
Accept SNMP Packets from all Host	Select this option if a query sent from any Manager terminal is valid. When selected, the Accept SNMP Packets from These Hosts option is disabled.	
Accept SNMP Packets from the following Hosts	Lists specific Manager terminals whose queries will be considered as valid. This option is enabled when the Accept SNMP Packets from any Host option is cleared.	
User Name	Enter a *User Name* of up to 48 characters **Default:** Empty	Version 3
Security Level	Select a *Security Level* from the drop-down menu. **Range:** *No Auth, No Priv; Auth, No Priv; Auth, Priv* **Default:** Auth, Priv	
Authentication Protocol	Select the authentication protocol **Range:** *MD5, SHA* **Default:** *MD5*	These fields are enabled if *Authentication* is selected in the *Security Level* field.
Authentication Password	Enter an *Authentication Password.* **Range:** 8 - 48 characters **Default:** Empty	
Privacy Protocol	Select a *Privacy Protocol*. **Range:** DES, AES **Default:** DES	
Privacy Password	Enter a *Privacy Password*. **Range:** 8 - 48 characters **Default:** Empty	These fields are enabled if *Privacy* is selected in the *Security Level* field.
Engine ID	Enter an *Engine ID* to be used for both the *Agent* and the *Trap*. **Default:** Empty	

16 To specifically define one or more valid terminals, ensure that the *Accept SNMP Packets from any Host* option is cleared and then click the **Add** button.

The *Accepted Host IP Address* dialog box opens.

17 Enter the *IP Address* of the Manager terminal from which valid queries may be sent to the MCU, and then click **OK**.
Click the **Add** button to define additional *IP Addresses*.
The *IP Address* or *Addresses* are displayed in the *Accept SNMP Packets from These Hosts* box.

> Queries sent from terminals not listed in the *Accept SNMP Packets from These Hosts* box are regarded as a violation of the MCU security, and if the *Send Authentication Trap* check box is selected, an appropriate message will be sent to all the terminals listed in the *SNMP Properties – Traps* dialog box.

18 In the *Collaboration Server - SNMP Properties - Security* dialog box, click **OK**.

Audible Alarms

In addition to the visual cues used to detect events occurring on the Collaboration Server, an audible alarm can be activated and played when participants request Operator Assistance.

Using Audible Alarms

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU in either the *Collaboration Server Web Client* or *RMX Manager*.

The Audible Alarm played when Operator Assistance is requested is enabled and selected in the **Setup > Audible Alarm > User Customization**. When the Audible Alarm is activated, the *.wav file selected in the *User Customization* is played, and it is repeated according to the number of repetitions defined in the *User Customization*.

If more than one Collaboration Server is monitored in the *RMX Manager*, the Audible Alarm must be enabled separately for each Collaboration Server installed in the site/configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, the Audible Alarms are synchronized and played one after the other. It is important to note that when *Stop Repeating Alarm* is selected from the toolbar from the *Collaboration Server Web Client* or *RMX Manager*, all activated Audible Alarms are immediately halted.

Audible Alarm Permissions

An operator/administrator can configure the Request Operator Assistance audible alarm, however Users with different authorization level have different configuration capabilities as shown in Table 19-16.

Table 19-16 Audible Alarm Permissions

Option	Operator	Administrator
User Customization	✔	✔
Download Audible Alarm File		✔
Stop Repeating Alarms	✔	✔

Stop Repeating Message

The Collaboration Server User can stop playing the audible alarm at any time. If more than one audible alarm has been activated, all activated alarms are immediately stopped.

If after stopping the Audible Alarms a new Operator Assistance request event occurs, the audible alarm is re-activated.

To stop the Audible Alarm on the Collaboration Server Client or RMX Manager:

>> On the Collaboration Server menu, click **Setup > Audible Alarms >Stop Repeating Alarm**.

When selected all audible alarms are immediately stopped.

Configuring the Audible Alarms

User Customization

The operators and administrators can:

*   Enable/Disable the Audible Alarm.
*   Select whether to repeat the Audible Alarm.
*   Define the number of repetitions and the interval between the repetitions.

To Customize the Audio Alert on the Collaboration Server Client or RMX Manager:

1 On the Collaboration Server menu, click **Setup > Audible Alarms > User Customization**.

The *User Customization* window opens.
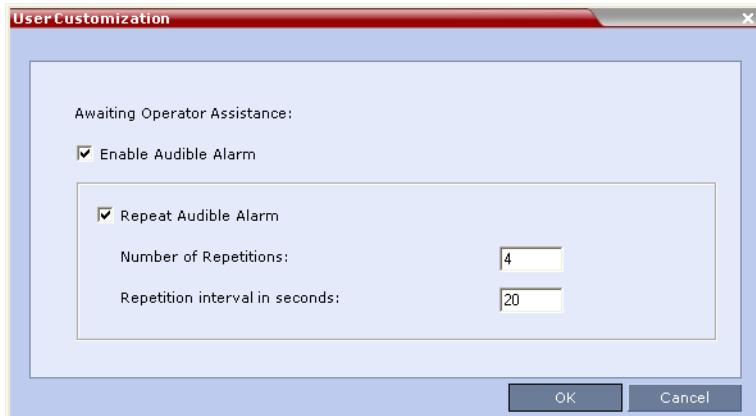
2 Define the following parameters:

Table 19-17 Audible Alarm - User Customization Options

Option	Description
Enable Audible Alarm	Select this check box to enable the Audible Alarm feature and to define its properties. When this check box is cleared, the Audible Alarm functionality is disabled.
Repeat Audible Alarm	Select this check box to play the Audible Alarm repeatedly. When selected, it enables the definition of the number of repetitions and the interval between repetitions. When cleared, the Audible Alarm will not be repeated and will be played only once.
Number of Repetitions	Define the number of times the audible alarm will be played. Default number of repetitions is 4.
Repetition interval in seconds	Define the number of seconds that the system will wait before playing the Audible Alarm again. Default interval is 20 seconds.

3 Click **OK**.

Replacing the Audible Alarm File

Each Collaboration Server is shipped with a default tone file in *.wav format that plays a specific tone when participants request Operator Assistance. This file can be replaced by a *.wav file with your own recording. The file must be in *.wav format and its length cannot exceed one hour.

Only the User with Administrator permission can download the Audible Alarm file.

To replace the Audio file on the Collaboration Server Client or RMX Manager:

1 On the Collaboration Server menu, click **Setup > Audible Alarms > Download Audible Alarm File**.
The *Download Audible Alarm File* window opens.

2 Click the **Browse** button to select the audio file (*.wav) to download.

The *Open* dialog box opens.
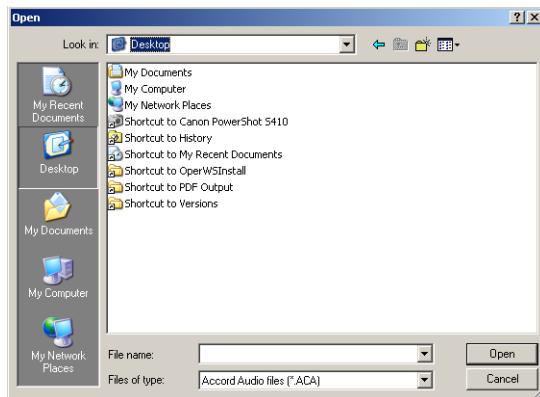
3 Select the appropriate *.wav file and then click the **Open** button.
The selected file name is displayed in the *Install Audible Alarm File* dialog box.

4 **Optional**. You can play the selected file or the currently used file by clicking the *Play* ( ) button as follows:

a Click **Play Selected File** to play a file saved on your computer.

b Click **Play Collaboration Server File** to play the file currently saved on the Collaboration Server.

5 In the *Download Audible Alarm File* dialog box, click **OK** to download the file to the MCU.

The new file replaces the file stored on the MCU. If multiple Collaboration Servers are configured in the *RMX Manager*, the file must be downloaded to each of the required MCUs separately.

Multilingual Setting

Each supported language is represented by a country flag in the *Welcome Screen* and can be selected as the language for the *Collaboration Server Web Client.*

Customizing the Multilingual Setting

The languages available for selection in the *Login* screen of the *Collaboration Server Web Client* can be modified using the *Multilingual Setting* option.

To customize the Multilingual Setting:

1 On the Collaboration Server menu, click **Setup > Customize Display Settings > Multilingual Setting**.

The *Multilingual Setting* dialog box is displayed.
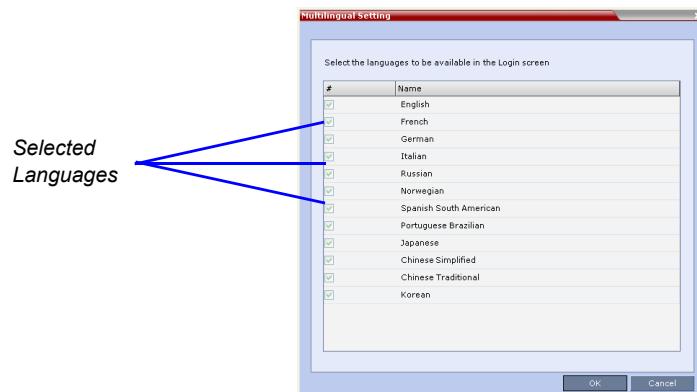
2 Click the check boxes of the languages to be available for selection.

3 Click **OK**.

4 **Log out** from the *Collaboration Server Web Client* and **Log in** for the customization to take effect**.**

Banner Display and Customization

The *Login Screen* and *Main Screen* of the *Collaboration Server Web Client* and the *Collaboration Server Manager can* display informative or warning text banners. These banners can include general information or they can be cautioning users to the terms and conditions under which they may log into and access the system, as required in many secured environments.

Banner display is enabled in the *Setup > Customize Display Settings > Banners Configuration*.

The administrator can choose one of four alternative login banners to be displayed. The four alternative banners cannot be modified. A *Custom* banner (default) can also be defined.

The *Main Page Banner* is blank and can be defined.

The *Banner Configuration* dialog box allows the administrator to select a *Login Banner* from a drop-down menu.
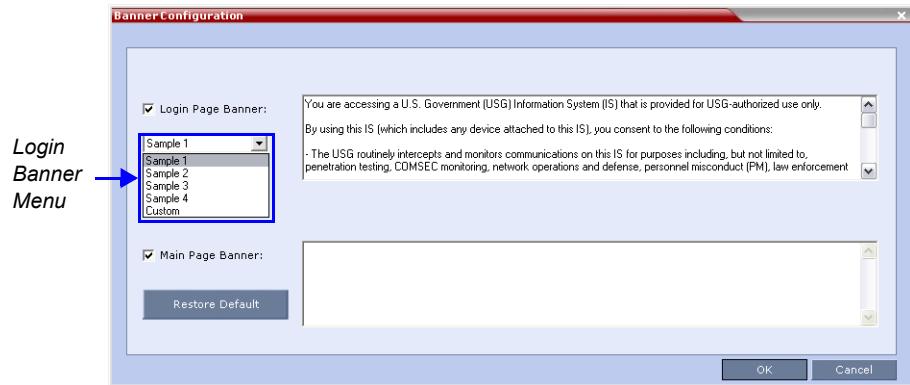
One of the the following *Login Banners* can be selected:

• **Non-Modifiable Banners**

— *Sample 1*

— *Sample 2*

— *Sample 3*

— *Sample 4*

• **Modifiable Banner**

— *Custom* (Default)

Guidelines

• The *Login Banner* must be acknowledged before the user is permitted to log in to the system.

• If a *Custom* banner has been created, and the user selects one of the alternative, non-modifiable banners the *Custom* banner not deleted.

• The *Custom Login Banner* banner may contain up to 1300 characters.

• An empty *Login Banner* is not allowed.

- Any attempt to modify a non-modifiable banner results in it automatically being copied to the *Custom* banner.

Non-Modifiable Banner Text

Sample 1 Banner

```
You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you
consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense,  personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be
disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or
privacy.
- Notwithstanding the above, using this IS does not constitute consent to
PM, LE or CI investigative searching or monitoring of the content of
privileged communications, or work product, related to personal
representation or services by attorneys, psychotherapists, or clergy, and
their assistants. Such communications and work product are private and
confidential. See User Agreement for details.
```

Sample 2 Banner

```
This system is for the use of authorized users only. Individuals using this
computer system without authority, or in excess of their authority, are
subject to having all of their activities on this system monitored and
recorded by systems personnel. In the course of monitoring individuals
improperly using this system, or in the course of system maintenance, the
activities of authorized users also may be monitored. Anyone using this
system expressly consents to such monitoring and is advised that if such
monitoring reveals possible criminal activity, system personnel may provide
the evidence of such monitoring to law enforcement officials.
```

Sample 3 Banner

```
You are about to access a system that is intended for authorized users only.
You should have no expectation of privacy in your use of this system.  Use
of this system constitutes consent to monitoring, retrieval, and disclosure
of any information stored within the system for any purpose including
criminal prosecution.
```

Sample 4 Banner

```
This computer system including all related equipment, network devices
(specifically including Internet access), is provided only for authorized
use. All computer systems may be monitored for all lawful purposes,
including ensuring that their use is authorized, for management of the
system, to facilitate protection against unauthorized access, and to verify
security procedures, survivability and operational security. Monitoring
```

```
includes active attacks by authorized personnel and their entities to test
or verify the security of the system. During monitoring, information may be
examined, recorded, copied and used for authorized purposes. All information
including personal information, placed on or sent over this system may be
monitored. Use of this system, authorized or unauthorized, constitutes
consent to monitoring of this system. Unauthorized use may subject you to
criminal prosecution. Evidence of any such unauthorized use collected during
monitoring may be used for administrative, criminal or other adverse action.
Use of this system constitutes consent to monitoring for these purposes.
```

Customizing Banners

The *Login* and *Main Screen* banners can be customized to display conference information, assistance information or warning text as required in the *Ultra Secure Mode*.

To customize the banners:

1 In the *Collaboration Server* menu, click **Setup > Customize Display Settings > Banners Configuration**.

The *Banners Configuration* dialog box opens.
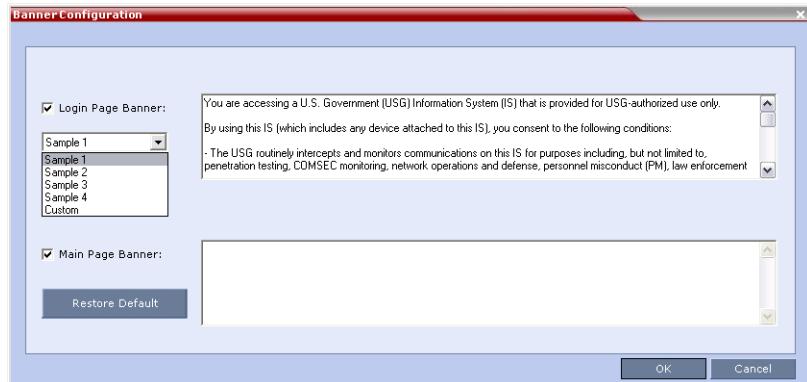
2 Customize the banners by modifying the following fields:

Table 19-18 Banner Configuration

Field	Description		
	Check Box	**Text Field**	**Restore Default Button**
Login Page Banner	Select or clear the check box to enable or disable the display of the banner.	Edit the text in this field to meet local requirements: • Banner content is multilingual and uses Unicode, UTF-8 encoding. All text and special characters can be used. • Maximum banner size is 100KB.	Click the button to restore the default text to the banner
Main Page Banner			

3 Click the **OK** button.

Banner Display

Login Screen Banner

The *Login* screen banner can display any text, for example the terms and conditions for system usage. The user must acknowledge that the information was read and click the **Accept** button to proceed to the *Login* screen as shown in the following screen:

Main Screen Banner

The *Main Screen* banner is displayed at the bottom of the screen, as follows:

Software Management

The *Software Management* menu is used to backup and restore the Collaboration Server's configuration files and to download MCU software.

Backup and Restore Guidelines

- *System Backup* can only be performed by an administrator.
- The *System Backup* procedure creates a single backup file that can be viewed or modified only by developers.
- A *System Backup* file from one system can be restored on another system.
- To ensure file system consistency, do not perform any configuration changes as the system does not suspended them during the backup procedure.
- The following parameters, settings and files are backed up:
  — MCMS configuration files (/mcms/Cfg):
  — Network and service configurations,
  — Rooms,
  — Profiles
  — Reservations
  — System Flags
  — Resource Allocation
  — IVR messages, music
  — *Collaboration Server Web Client* user setting - fonts, windows
  — *Collaboration Server Web Client* global settings – notes, address book, language
  — Private keys and certificates (TLS)
  — Conference participant settings
  — Operation DB (administrator list)
  — SNMP settings
  — Time configuration

- CDR files are not included in the backup process and should be backed up manually by saving the CDR files to a destination device.

Using Software Management

To backup configuration files:

1   On the *Collaboration Server* menu, click **Administration > Software Management > Backup Configuration**.

The *Backup Configuration* dialog box opens.
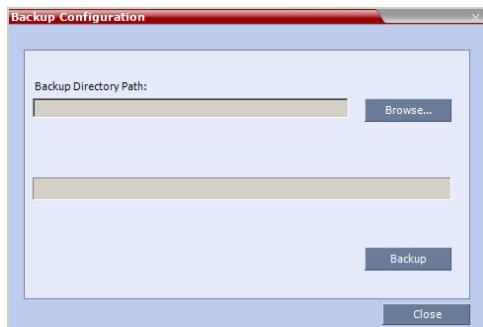
2   **Click the Browse** button.
The Browse To File dialog box opens.

3   Select the *Backup Directory Path* and then click **Backup**.

> When the Collaboration Server system backs up the current configuration, if any changes occur immediately or during the request, then additional changes are not registered.

To restore configuration files:

1   On the *Collaboration Server* menu, click **Administration > Software Management > Restore Configuration**.

2   **Browse** to the *Restore Directory Path* where the backed up configuration files are stored and then click **Restore**.

To download MCU software files:

1   On the *Collaboration Server* menu, click **Administration > Software Management > Software Download**.

2   **Browse** to the *Install Path* and then click **Install**.

Ping Collaboration Server

The *Ping* administration tool enables the *Collaboration Server Signaling Host* to test network connectivity by *Pinging* IP addresses.

Guidelines

- Both explicit IP addresses and *Host Names* are supported.

- The *Collaboration Server Web Client* blocks any attempt to issue another *Ping* command before the current *Ping* command has completed. Multiple *Ping* commands issued simultaneously from multiple *Collaboration Server Web Client*s are also blocked.

Using Ping

To Ping a network entity from the *Collaboration Server*:

1 On the *Collaboration Server* menu, click **Administration > Tools > Ping**.

The *Ping* dialog box is displayed:
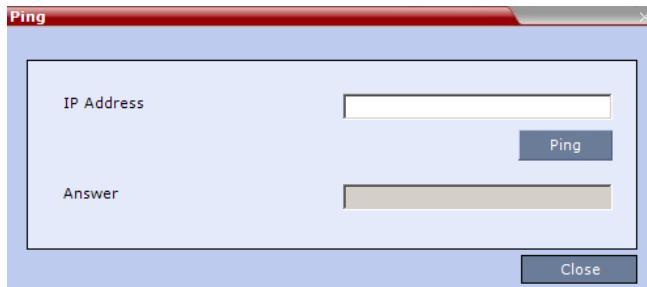
2 Modify or complete the following field:

Table 19-19 Ping

Field	Description
Host Name or Address	Enter the *Host Name* or *IP Address* of the *network* entity to be *Pinged*.

3 Click the **Ping** button.

The *Ping* request is sent to the *Host Name* or *IP Address* of the *Collaboration Server* entity.

The *Answer* is either:

— *OK, or*
— *FAILED*

Notification Settings

The Collaboration Server can display notifications when:

- A new Collaboration Server user connects to the MCU.
- A new conference is started.
- Not all defined participants are connected to the conference or when a single participant is connected.
- A change in the MCU status occurs and an alarm is added to the alarm's list.

A welcome message is displayed to the Collaboration Server user upon connection.

To configure the notifications:

1 On the *Collaboration Server* menu, select **Setup > Notification Settings**.

The *Notification Settings* dialog box is displayed.
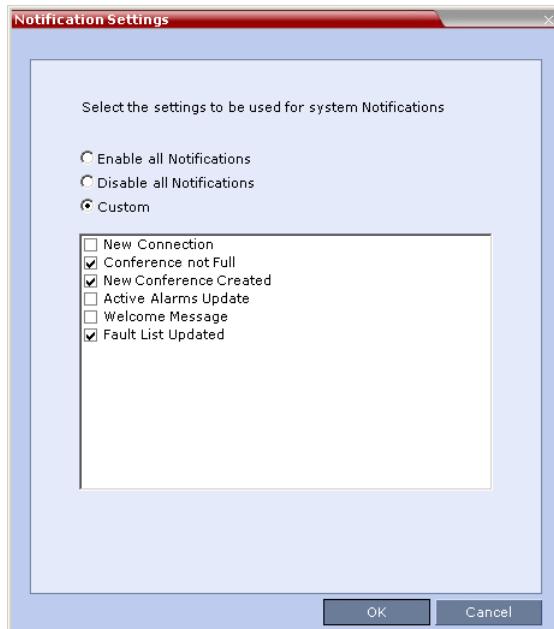
The following notification options are displayed.

Table 19-20 Notification Settings Parameters

Field	Description
New Connection	Notification of a new user/administrator connecting to the Collaboration Server.
New Conference Created	New conference has been created.
Conference Not Full	The conference is not full and additional participants are defined for the conference.
Welcome Message	A welcome message after user/administrator logon.
Active Alarms Update	Updates you of any new alarm that occurred.
Fault List Updated	Updates you when the faults list is updated (new faults are added or existing faults are removed).

2 **Enable/Disable All Notifications** or **Custom** to select specific notifications to display.

3 Click **OK**.

Logger Diagnostic Files

The Logger utility is a troubleshooting tool that continually records MCU system messages and saves them to files in the MCU hard drive. For each time interval defined in the system, a different data file is created. The files may be retrieved from the hard drive for off-line analysis and debugging purposes.

The Logger utility is activated at the MCU startup. The Logger is disabled when the MCU is reset manually or when there is a problem with the Logger utility, e.g. errors on the hard drive where files are saved. In such cases, data cannot be retrieved.

When the MCU is reset via the Collaboration Server, the files are saved on the MCU hard drive.

To access the Logger Diagnostic Files:

>> On the *Collaboration Server* menu, click **Administration > Tools > Logger Diagnostic Files**.
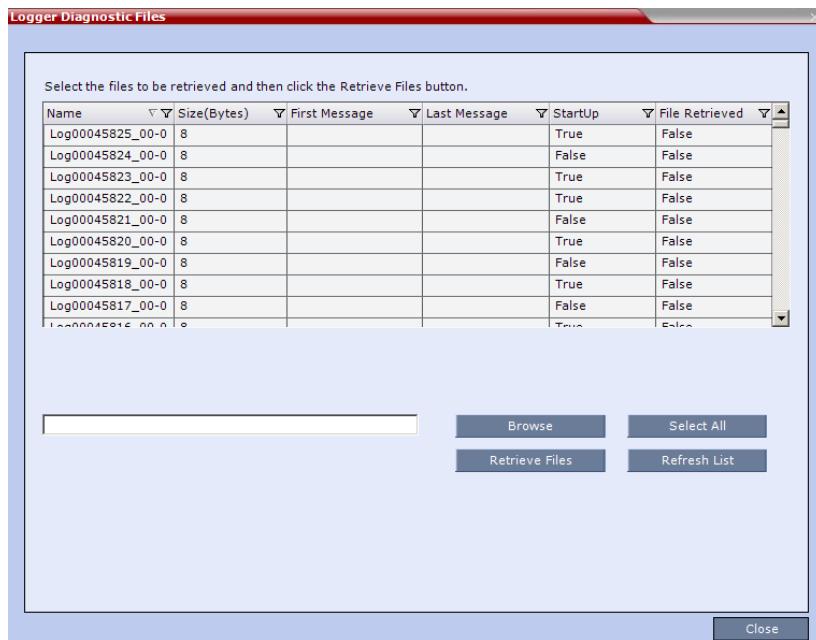
The following tasks can be performed:

Table 19-21 Diagnostic File Button Options

Button	Description
Refresh List	Refreshes the list and adds newly generated logger files.
Select All	Selects all the logger files listed.
Browse	Selects the destination folder for download.
Retrieve Files	Saves files to the destination folder.

When retrieved, the log file name structure is as follows:

• Sequence number (starting with 1)
• Date and Time of first message

- Date and Time of last message
- File size
- Special information about the data, such as Startup

File name structure:

Log_SNxxxxxxxxxx_FMDddmmyyy_FMThhmm_LMDddmmyyyy_LMThhmm_SZxxxxxxxxxx_SUY.log

File name format:

- SN = Sequence Number
- FM = First Message, date and time
- LM = Last Message, date and time
- SZ = Size
- SU = Startup (Y/N) during the log file duration

Example:

Log_SN0000000002_FMD06032007_FMT083933_LMD06032007_LMT084356_SZ184951_SUY.log.

Retrieving the Logger Files:

1   Select the log files to retrieve. Multiple selections of files are enabled using standard Windows conventions.

2   In the *Logger Diagnostic Files* dialog box, click the **Browse** button.

3   In the *Browse for Folder* window, select the directory location to save the Logger files and click **OK**.

    You will return to the *Logger Diagnostic Files* dialog box.

4   Click the **Retrieve Files** button.

    The log files (in *.txt format) are saved to the defined directory and a confirmation caption box is displayed indicating a successful retrieval of the log files.

Viewing the Logger Files:

To analyze the log files generated by the system, open the retrieved *.txt files in any text editor application, i.e. Notepad, Textpad or MS Word.

1   Using Windows Explorer, browse to the directory containing the retrieved log files.

2   Use any text editor application to open the log file(s).

Information Collector

Standard Security Mode

The Information Collector comprehensively attains all information from all the MCU internal entities for data analysis. That data, stored in a central repository, is logged from the following system components:

- System Log Files
- CDR

- Full faults
- Apache logs

- OS (Core dumps, CFG - DNS, DHCP, NTP, kernal state, event logs
- CFG directory (without IVR)
- Signaling Trace files (H.323 & SIP)
- Cards info: HW version, state and status
- Central Signaling logs
- SW version number
- Processes internal state and statistics

The data collected is saved into a single compressed file containing all the information from each system component in its relative format (.txt, .xml, etc...). In case the disk is malfunctioning, the file will be written to the RAM (involves only a small amount of information where the RAM size is 1/2 a gigabyte). The zipped file (info.tgz) can be opened with the following applications: WinRAR and WinZip. The entire zipped file is then sent to Polycom's Network Systems Division for analysis and troubleshooting.

Using the Information Collector

When the *Information Collector* is used the following steps are performed:

- **Step 1: Creating** the *Information Collector* file.
- **Step 2**: **Saving** the *Information Collector* file.
- **Step 3: Viewing** the information in the *Information Collector* file.

Step 1: Creating the Information Collector Compressed File

To create the compressed file:

1 In the Collaboration Server menu, click **Administration > Tools > Information Collector**.

   The *Information Collector* dialog box is displayed.

   Standard Security Mode
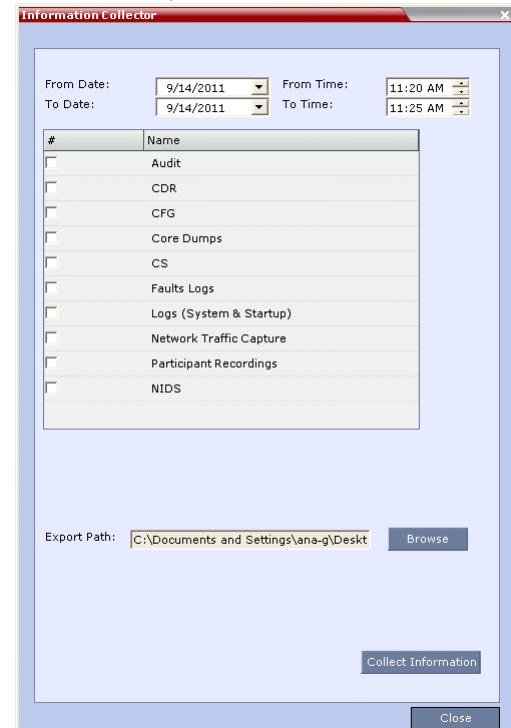
2 In the *From Date* and *Until Date* fields, use the arrow keys to define the date range of the data files to be included in the compressed file.

3 In the *From Time* and *Until Time* fields, use the arrow keys to define the time range of the data files to be included in the compressed file.

> If logs are being collected in order to troubleshoot a specific issue, it is important that the date and time range include the time and date in which the issue occurred. The default date and time ranges may not be sufficient.
> For example, if a specific issue occurred on October 1, 2013 at 12:15, the *From Date* and *Until Date* should be October 1, 2013, the *From Time* should be around 12:10, and the *Until Time* should be around 12:20.

4 Select check boxes of the information to be collected.

5 In the *Export Path* field, click the **Browse** button and navigate to the directory path where the compressed file is to be saved.

6 Click the **Collect Information** button.

   A progress indicator is displayed in the *Information Collector* dialog box while the file is being created.

Step 2: Saving the Compressed File

1 The compressed file is automatically saved in the directory selected in the *Information Collector* dialog box. The file is named **info.tgz**.

A success information box is displayed.

2 Click the **OK** button.

Step 3: Viewing the Compressed File

The compressed file is saved in *.tgz* format and can be viewed with any utility that can open files of that format, for example *WinRAR® 3.80*.

To view the compressed file:

1 Navigate to the directory on the workstation in which the file was saved.

2 Double click the **info.tgz** file to view the downloaded information.

> Some browsers save the file as *info.gz* due to a browser bug. If this occurs, the file must be manually renamed to *info.tgz* before it can be viewed.

Auditor

An *Auditor* is a user who can view *Auditor* and *CDR* files for system auditing purposes.

> The *Auditor* user must connect to the *Collaboration Server* using the *Collaboration Server Web Client* only.

The *Event Auditor* enables administrators and auditors to analyze configuration changes and unusual or malicious activities in the *Collaboration Server* system.

Auditor operates in real time, recording all administration activities and login attempts from the following *Collaboration Server* modules:

• Control Unit

• Shelf Manager

For a full list of monitored activities, see Table 19-23 on page **19-49** and Table 19-24 on page **19-51**.

The *Auditor* must always be active in the system. A *System Alert* is displayed if it becomes inactive for any reason.

The *Auditor* tool is composed of the *Auditor Files* and the *Auditor File Viewer* that enables you to view the *Auditor Files*.

> Time stamps of *Audit Events* are GMT.

Auditor Files

Auditor Event History File Storage

All audit events are saved to a buffer file on hard disk in real time and then written to a file on hard disk in XML in an uncompressed format.

A new current auditor event file is created when:

- the system is started
- the size of the current auditor event file exceeds 2 MB
- the current auditor event file's age exceeds 24 hours

Up to 1000 auditor event files are stored per *Collaboration Server*. These files are retained for at least one year and require 1.05 GB of disk space. The files are automatically deleted by the system (oldest first) when the system reaches the auditor event file limit of 1000.

A *System Alert* is displayed with *Can't store data* displayed in its *Description* field if:

- the system cannot store 1000 files
- the *Collaboration Server* does not have available disk space to retain files for one year

Audit Event Files are retained by the *Collaboration Server* for at least 1 year. Any attempt to delete an audit event file that is less than one year old raises a *System Alert* with *File was removed* listed in the *Description* field.

Using the *Restore Factory Defaults* of the *System Restore* procedure erases *Audit Files*.

Retrieving Auditor Files

You can open the *Auditor* file directly from the *Auditor Files* list or you can retrieve the files and save them to a local workstation.

To access Auditor Files:

>> On the *Collaboration Server* menu, click **Administration > Tools > Auditor Files**.

The *Auditor Files* dialog box is displayed.
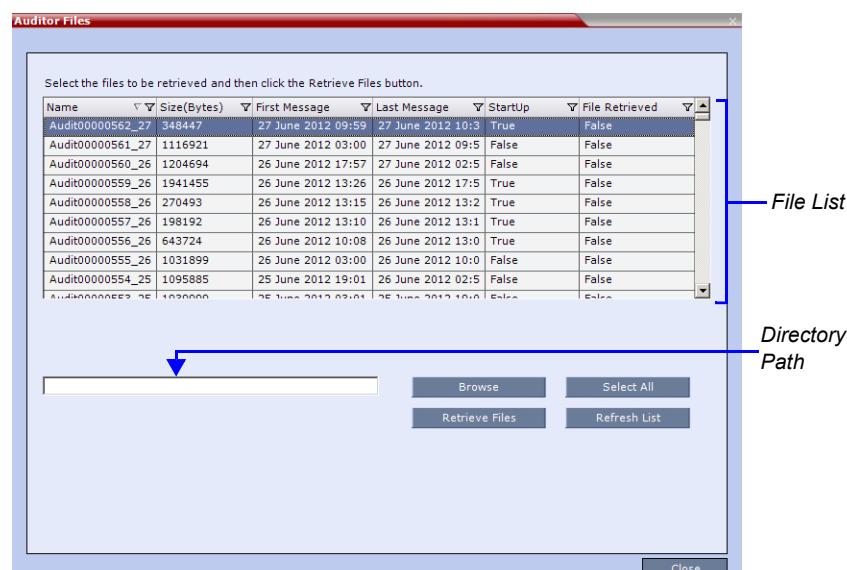
The *Auditor Files* dialogue box displays a file list containing the following file information:

— *Name*
— Size (Bytes)
— *First Message* – date and time of the first audit event in the file
— *Last Message* – date and time of the last audit event in the file
— StartUp:
  - *True* – file was created when the system was started

- *False* – file was created when previous audit event file reached a size of 2 MB or was more than 24 hours old
— File Retrieved:
  - *True* - file was previously retrieved.
  - *False* - file was never previously retrieved.

The order of the *Auditor Files* dialog box field header columns can be changed and the fields can be filtered to enable searching.

For more information, see "*Auditor File Viewer*" on page **19-47**.

To retrieve files for storage on a workstation:

1   Click **Browse** and select the folder on the workstation to receive the files and then click **OK**.

The folder name is displayed in the directory path field.

2   Select the file(s) to be retrieved by clicking their names in the file list or click **Select All** to retrieve all the files. (Windows multiple selection techniques can be used.)

3   Click Retrieve Files.

The selected files are copied to the selected directory on the workstation.

To open the file in the Auditor File Viewer:

>>   Double-click the file.

Auditor File Viewer

The *Auditor File Viewer* enables *Auditors* and *Administrators* to view the content of and perform detailed analysis on auditor event data in a selected *Auditor Event File*.

You can view an *Auditor Event File* directly from the *Auditor Files* list or by opening the file from the *Auditor File Viewer*.

To open the Auditor File Viewer from the Administration Menu:

1   On the *Collaboration Server* menu, click **Administration > Tools > Auditor File Viewer**.

The *Auditor File Viewer* is displayed.

If you previously double clicked an *Auditor Event File* in the *Auditor Files* list, that file is automatically opened.

Local File

Event List (ID)   *Request Transaction Tree*   *Response Transaction Tree*

The following fields are displayed for each event:

Table 19-22 *Auditor Event Columns*

Field	Description
Event ID	The sequence number of the event generated by the *Collaboration Server*.
Date & Time	The date and time of the event taken from the *Collaboration Server*'s *Local Time* setting.
User Name	The *Username* (Login Name) of the user who triggered the event.
Reporting Module	The *Collaboration Server* system internal module that reported the event: • MCMS • MPL • Central Signaling • MPL Simulation • *Collaboration Server* Web Client • CM Switch • ART • Video • MUX
Workstation	The name (alias) of the workstation used to send the request that triggered the event.
IP Address (Workstation)	The IP address of the workstation used to send the request that triggered the event.
Event Type	Auditor events can be triggered by: • API • HTTP • *Collaboration Server* Internal Event
Event	The process, action, request or transaction that was performed or rejected. • POST:SET transactions (API) • Configuration changes via XML (API) • Login/Logout (API) • GET (HTTP) • PUT (HTTP) • MKDIR (HTTP) • RMDIR (HTTP) • Startup (*Collaboration Server* Internal Event) • Shutdown (*Collaboration Server* Internal Event) • Reset (*Collaboration Server* Internal Event) • Enter Diagnostic Mode (*Collaboration Server* Internal Event) • IP address changes via USB (*Collaboration Server* Internal Event)

Table 19-22 Auditor Event Columns (Continued)

Field	Description
Process Completed	Status of the process, action, request or transaction returned by the system: • Yes – performed by the system. • No – rejected by the system.
Description	A text string describing the process, action, request or transaction.
Additional Information	An optional text string describing the process, action, request or transaction in additional detail.

The order of the *Auditor File Viewer* field header columns can be changed and the fields can be sorted and filtered to facilitate different analysis methods.

2   In the event list, click the events or use the keyboard's Up-arrow and Down-arrow keys to display the *Request Transaction* and *Response Transaction* XML trees for each audit event.

The transaction XML trees can be expanded and collapsed by clicking the expand (⊞) and collapse (⊟) buttons.

To open an auditor event file stored on the workstation:

1   Click the **Local File** button (📁) to open the *Open* dialogue box.

2   Navigate to the folder on the workstation that contains the audit event file.

3   Select the audit event file to be opened.

4   Click **Open**.

The selected file is opened in the *Auditor Viewer*.

Audit Events

Alerts and Faults

Table 1 lists *Alerts* and *Faults* that are recorded by the *Auditor*.

Table 19-23 Alerts and Faults

Event
Attempt to exceed the maximum number of management session per user
Attempt to exceed the maximum number of management sessions per system
Central Signaling indicating Recovery status.
Failed login attempt
Failed to open Apache server configuration file.
Failed to save Apache server configuration file.
Fallback version is being used.

Table 19-23 Alerts and Faults *(Continued)*

Event
File system scan failure.
File system space shortage.
Internal MCU reset.
Internal System configuration during startup.
Invalid date and time.
Invalid MCU Version.
IP addresses of Signaling Host and Control Unit are the same.
IP Network Service configuration modified.
IP Network Service deleted.
Login
Logout
Management Session Time Out
MCU Reset to enable Diagnostics mode.
MCU reset.
Music file error.
New activation key was loaded.
New version was installed.
NTP synchronization failure.
Polycom default User exists.
Private version is loaded.
Restoring Factory Defaults.
Secured SIP communication failed.
Session disconnected without logout
SSH is enabled.
System Configuration modified.
System is starting.
System Resets.
TCP disconnection
Terminal initiated MCU reset.
The Log file system is disabled.

Table 19-23 Alerts and Faults (Continued)

Event
The software contains patch(es).
USB key used to change system configuration.
User closed the browser
User initiated MCU reset.

Transactions

Table 2 lists *Transactions* that are recorded by the *Auditor*.

Table 19-24 Transactions

Transaction
TRANS_CFG:SET_CFG
TRANS_IP_SERVICE:DEL_IP_SERVICE
TRANS_IP_SERVICE:NEW_IP_SERVICE
TRANS_IP_SERVICE:SET_DEFAULT_H323_SERVICE
TRANS_IP_SERVICE:SET_DEFAULT_SIP_SERVICE
TRANS_IP_SERVICE:UPDATE_IP_SERVICE
TRANS_IP_SERVICE:UPDATE_MANAGEMENT_NETWORK
TRANS_MCU:BEGIN_RECEIVING_VERSION
TRANS_MCU:COLLECT_INFO
TRANS_MCU:CREATE_DIRECTORY
TRANS_MCU:FINISHED_TRANSFER_VERSION
TRANS_MCU:LOGIN
TRANS_MCU:LOGOUT
TRANS_MCU:REMOVE_DIRECTORY
TRANS_MCU:REMOVE_DIRECTORY_CONTENT
TRANS_MCU:RENAME
TRANS_MCU:RESET
TRANS_MCU:SET_PORT_CONFIGURATION
TRANS_MCU:SET_RESTORE_TYPE
TRANS_MCU:SET_TIME
TRANS_MCU:TURN_SSH
TRANS_MCU:UPDATE_KEY_CODE

Table 19-24 *Transactions (Continued)*

Transaction
TRANS_OPERATOR:CHANGE_PASSWORD
TRANS_OPERATOR:DELETE_OPERATOR
TRANS_OPERATOR:NEW_OPERATOR
TRANS_SNMP:UPDATE

ActiveX Bypass

At sites that, for security reasons, do not permit Microsoft® ActiveX® to be installed, the MSI (Windows Installer File) utility can be used to install .NET Framework and .NET Security Settings components on workstations throughout the network.

All workstation that connect to *Collaboration Server* systems must have both .NET Framework and .NET Security Settings running locally. These components are used for communication with the Collaboration Server and can only be installed on workstations by users with administrator privileges.

The MSI utility requires the IP addresses of all the Collaboration Server systems (both control unit and Shelf Management IP addresses) that each workstation is to connect to. If the IP address of the any of the target Collaboration Servers is changed, the ActiveX components must be reinstalled.

Installing ActiveX

To install ActiveX components on all workstations in the network:

1 Download the MSI file **EMA.ClassLoaderInstaller.msi** from the Polycom Resource Center.
   The MSI file contains installation scripts for both .NET Framework and .NET Security Settings.

2 Create a text file to be used during the installation containing the IP addresses of all the Collaboration Server systems (both control unit and Shelf Management IP addresses) that each workstation in the network is to connect to.

   The file must be named **url_list.txt** and must be saved in the same folder as the downloaded MSI file.
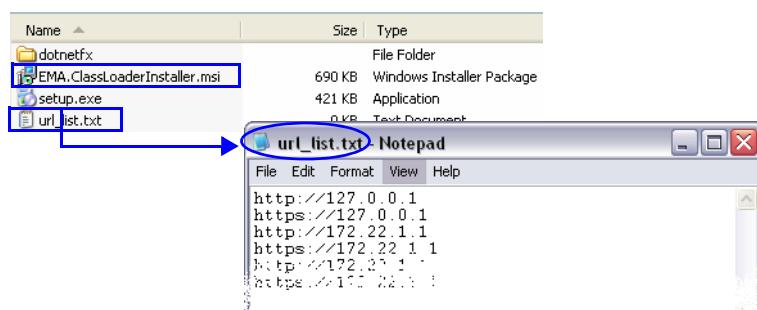
3 Install the ActiveX components on all workstations on the network that connect to Collaboration Server systems.

The installation is done by the network administrator using a 3rd party network software installation utility and is transparent to all other users.

Resetting the Collaboration Server (RMX)

System Reset saves system configuration changes and restarts the system with the latest settings.

To reset the RMX:

1 In the *RMX Management* pane, click the **Hardware Monitor button**.

The *Hardware Monitor* pane is displayed.

2 Click the **Reset** () button.
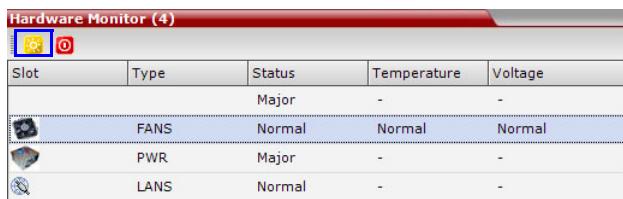
When the Collaboration Server system is reset, during Collaboration Server startup the *Progress Bar* appears at the bottom of the Collaboration Server *Status* pane.
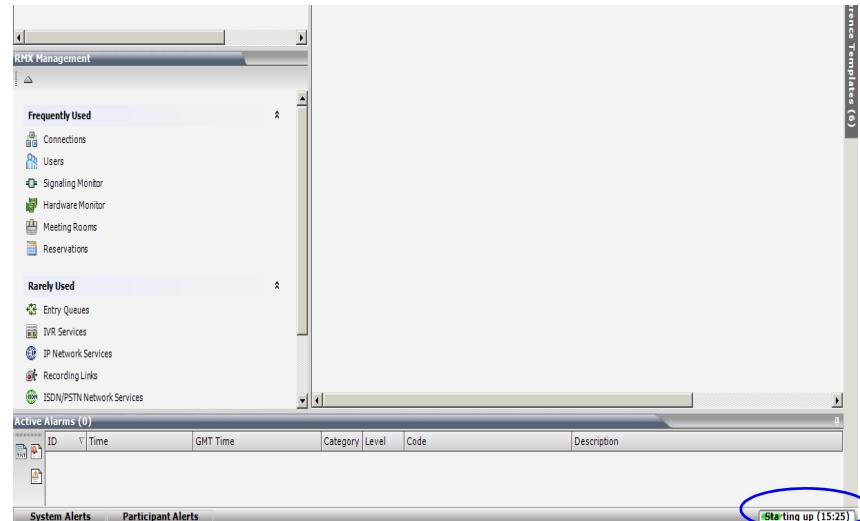
The progress bar displays the amount of time remaining for the reset process to complete: . The *Startup* progress is also indicated by a green bar moving from left to right.

The duration of the *Startup* depends on the type of activity that preceded the MCU reset. For example: Fast Configuration Wizard, New Version installation, Version Upgrade, Restore Last Configuration etc.

> When resetting the Collaboration Server from the Hardware Monitor, sometimes SIP endpoints may remain connected, although the conference ended.

This procedure allows an administrator to update the MCU instance without requiring the administrator to reregister the product.

> Updating the MCU instance requires the previously used activation key. If you no longer have the activation key, contact support before starting this procedure.

To update the MCU instance:

1 On the *Collaboration Server* menu, click **Administration > Software Management > Backup Configuration**.

The *Backup Configuration* dialog box opens.

2 **Click the Browse** button.
The Browse To File dialog box opens.

3 Select the *Backup Directory Path* and then click **Backup**.

> When the *Collaboration Server* backs up the current configuration, if any changes occur immediately or during the request, then additional changes are not registered.

After a few minutes, the MCU turns on.

4 Start the *Collaboration Server Web Client* application on the workstation.

a In the browser's address line, enter the IP address of the *Control Unit* in the format:
`http://<Control Unit IP Address>`.

b Click **Enter**.

The *Collaboration Server Web Client* Login screen is displayed.
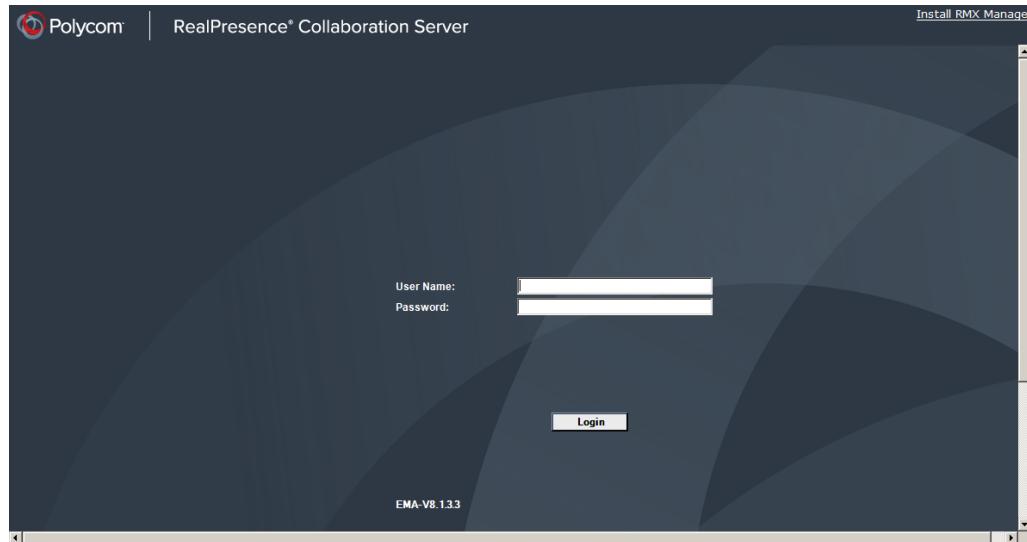
5 In the *Collaboration Server Web Client* Login screen, enter the default *Username* (**POLYCOM**) and *Password* (**POLYCOM**) and click **Login**.

The *Collaboration Server Web Client* opens and the *Product Activation* dialog box appears with the serial number filled in:
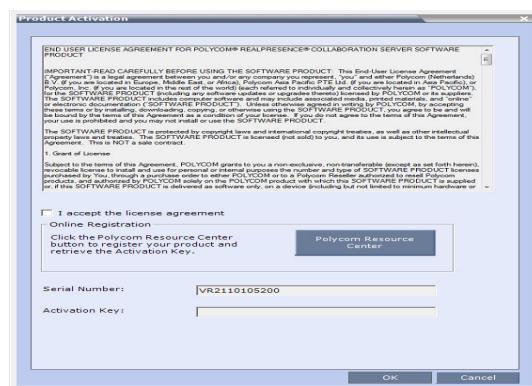
6 In the *Activation Key* field, enter or **paste** the *Product Activation Key*.

7 Click **OK.**
A message indicating that the *Product Activation Key* was loaded successfully appears. If the *Product Activation Key* fails to load, please contact your vendor.

8 Click **OK**.

> If the *Product Activation* dialog box does not appear, go to **Setup --> Product Activation** to display the dialog box.

9 On the *Collaboration Server* menu, click **Administration > Software Management > Restore Configuration**.

10 **Browse** to the *Restore Directory Path* where the backed up configuration files are stored and then click **Restore**.

20

System Configuration Flags

The system's overall behavior can be configured by modifying the default values of the System Flags.

> • For flag changes (including deletion) to take effect, the MCU must be reset. For more information, see "*Resetting the Collaboration Server (RMX)*" on page **19-54**.
> • ENABLE_SELECTIVE_MIXING

Modifying System Flags

To modify system flags:

1 On the *Collaboration Server* menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.
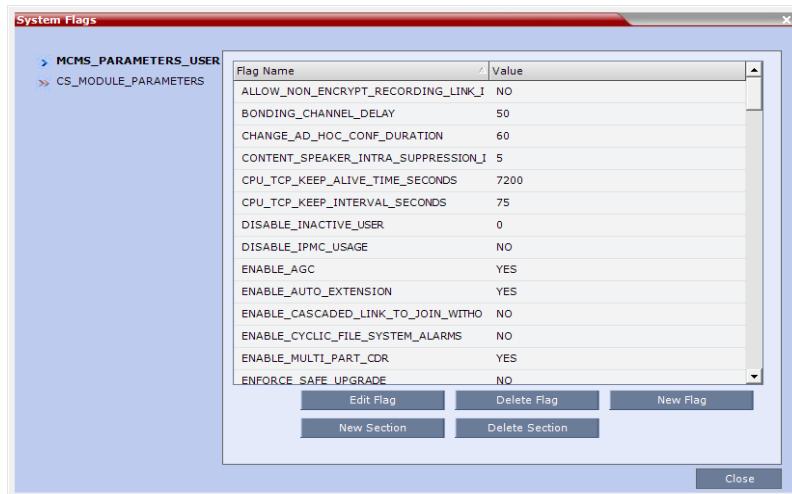
2 In the *MCMS_PARAMETERS* tab, the following flags can be modified:

Table 20-1 System Flags – MCMS_PARAMETERS

Flag	Description
ALLOW_NON_ENCRYPT_P ARTY_IN_ENCRYPT_CONF	If YES, allows non-encrypted participants to connect to encrypted conferences. Default: No

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	When set to **NO** (default), the Recording Link inherits the encryption settings of the conference. If the conference is encrypted, the recording link will be encrypted. When set to **YES**, it disables the encryption of the recording link, regardless of the Encryption settings of the conference and RSS recorder.
CHANGE_AD_HOC_CONF_DURATION	The duration of an ad-hoc conference* can be configured on a system level by setting the flag to one of the following values (in minutes): **60** (default), **90**, **180** and **270**. * An ad-hoc conference is automatically created when the participant dials into an Ad-hoc Entry Queue and enters a conference ID that is not being used by any other conferencing entity. It is based on the Conference Profile assigned to the EQ.
CONTENT_SLAVE_LINKS_INTRA_SUPPRESSION_IN_SECONDS	Defines the interval, in seconds, during which the Collaboration Server is allowed to forward an *Intra Request* received from any of the *Slave Cascading Links.* The *Slave Cascading Link* can be connected to the local Collaboration Server, to an MCU on a higher cascade level or to the *Content* sharer. The first *Intra* request that is received from any of the *Slave MCUs* connected to the Collaboration Server starts the interval counter and is forwarded to the next level *MCU* or to the *Content* sharer. All other *Intra* requests that are received within this interval are registered but ignored. After an interval of <flag value> seconds, the system checks if during the last interval any additional *Intra* requests were registered. If there is at least one *Intra* request it will be forwarded. If there is no additional *Intra* request not no action is taken other than to wait for the next cycle. This filtering process is repeated every <flag value> seconds. **Default:** 30
CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS	This flag controls the requests to refresh (intra) the content sent from the Collaboration Server system to the content sender as a result of refresh requests initiated by other conference participants. Enter the interval in seconds between the Intra requests sent from the Collaboration Server to the endpoint sending the content to refresh the content display. Refresh requests that will be received from endpoints within the defined interval will be postponed to the next interval. Default setting: 5

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
CPU_TCP_KEEP_ALIVE_TIME_SECONDS	This flag indicates when to send the first KeepAlive indication to check the TCP connection. Default value: **7200** second (120 minutes) Range: 600-18000 seconds When there are NAT problems, this default may be too long and the TCP connection is lost. In such a case, the default value should be changed to 3600 seconds (60 minutes) or less.
CPU_TCP_KEEP_INTERVAL_SECONDS	This flag indicates the interval in seconds between the KeepAlive requests. Default value: **75** second Range: 10-720 seconds.
DISABLE_INACTIVE_USER	Users can be automatically disabled by the system when they do not log into the Collaboration Server application for a predefined period. Possible Values: **0** - **90** days. Default: **0** (disables this option).
ENABLE_ACCEPTING_ICMP_REDIRECT	When set to YES, allows the RMX to accept *ICMP Redirect Messages (ICMP* message type #5). For more information see "*Internet Control Message Protocol (ICMP)"* on page **23-51** Possible values: YES / NO • Default: YES
ENABLE_AGC	Set this flag to YES to enable the AGC option. (Default setting is NO.) When disabled, selecting the AGC option in the *Participant Properties* has not effect on the participant audio. For more information see "*Managing the Address Book"* on page **8-7**. The Auto Gain Control mechanism regulates noise and audio volume by keeping the received audio signals of all participants balanced. **Note:** Enabling AGC may result in amplification of background noise.

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
ENABLE_AUTO_EXTENSION	When set to YES, allows conferences running on the Collaboration Server to be automatically extended as long as there are participants connected and the system has free resources. Set this flag to NO prevent conference duration from being automatically extended. It can also be used to enable the definition of conference duration that is shorter than is 11 minutes. Default: YES **Note:** If this flag is set to: • YES, *Gateway Calls* are not limited in duration while endpoints are connected. • NO, *Gateway Calls* are limited to 60 minutes. For more information see the *"Gateway Functionality"* on page **19-1**.
ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD	Enables a cascaded link to enter a conference without a password. Default: NO, for security reasons.
ENABLE_CYCLIC_FILE_SYSTEM_ALARMS	Enables or disables the display of Active Alarms before overwriting the older CDR/Auditor/Log files, enabling the users to backup the older files before they are deleted. Default: NO
ENFORCE_SAFE_UPGRADE	When set to YES this flag enables the Collaboration Server system to notify users when an incorrect version upgrade/downgrade or upgrade/downgrade path is selected. When set to NO, after initiating an upgrade or downgrade software installation, the Collaboration Server activates a fault alert in the Faults List: "Warning: Upgrade started and SAFE Upgrade protection is turned OFF" and the upgrade/downgrade process continues. Range: YES / NO Default: YES
ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE	
FORCE_CIF_PORT_ALLOCATION	Sets the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters. You can specify the endpoint types for which resource allocation can be forced to CIF resource, enabling other types of endpoints to use higher resolutions in the same conference. Enter the product type to which the CIF resource should be allocated. Possible values are: • **CMA Desktop -** for CMA desktop client • **VSX nnnn** - where nnnn represents the model number for example, VSX 8000.

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
GK_MANDATORY_FOR_CALLS_IN	If set to **YES**, a gatekeeper is required to receive incoming H.323 calls. If a gatekeeper is not configure in the Collaboration Server, the calls will fail. If set to **NO** (default), gatekeeper is not required to process H.323 incoming calls and H.323 participants can dial in with or without a gatekeeper.
GK_MANDATORY_FOR_CALLS_OUT	If set to **YES**, a gatekeeper is required to perform H.323 outgoing calls. If a gatekeeper is not configure on the Collaboration Server, the calls will fail. If set to **NO** (default), gatekeeper is not required to dial out to H.323 participants and calls can be dialed out with or without a gatekeeper.
H263_ANNEX_T	Set to NO to send the content stream without Annex T and enable Aethra and Tandberg endpoints, that do not support Annex T, to process the content. Default: YES
HD_THRESHOLD_BITRATE	Sets the minimum bit rate required by endpoints to connect to an HD Conference. Endpoints that cannot support this bit rate are connected as audio only. Range: 384kbps - 4Mbs (Default: 768)
MAX_CONF_PASSWORD_REPEATED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a conference password. Range: 1 - 4 Default: 2
MAX_CP_RESOLUTION	The MAX_CP_RESOLUTION flag value is applied to the system during *First Time Power-on* and after a system upgrade. The default value is . All subsequent changes to the Maximum CP Resolution of the system are made using the *Resolution Configuration* dialog box. Possible flag values: • **HD1080** - High Definition at 60 fps • **HD720** – High Definition at 60 fps • **HD** – High Definition at 30 fps • **SD30** – Standard Definition at 30 fps • **SD15** – Standard Definition at 15 fps • **CIF** – CIF resolution Default: HD1080 For more information see "*Video Resolutions in AVC-based CP Conferencing"* on page **4-1**. **Note:** From Version 8.1, MPM+ media card is not supported.

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
*MAX_INTRA_REQUESTS_PER_INTERVAL_*	Enter the maximum number of refresh (intra) requests for the Content channel sent by the participant's endpoint in a 10 seconds interval that will be dealt by the Collaboration Server system. When this number is exceeded, the Content sent by this participant will be identified as noisy and his/her requests to refresh the Content display will be suspended. Default setting: 3
*MAX_INTRA_SUPPRESSION_DURATION_IN_SECONDS_*	Enter the duration in seconds to ignore the participant's requests to refresh the Content display. Default setting: 10
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM	Defines the maximum number of concurrent management sessions (http and https connections) per system. Value: 4 - 80 Default: 80
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER	Defines the maximum number of concurrent management sessions (http and https connections) per user. Value: 4 - 80 Default: 10
MAX_PASSWORD_REPEAPED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a user password. Range: 1 - 4 Default: 2
MCU_DISPLAY_NAME	The name of the MCU that is displayed on the endpoint's screen when connecting to the conference. Default: POLYCOM RealPresence Collaboration Server 1800
MIN_SYSTEM_DISK_SPACE_TO_ALERT	Defines a minimum remaining Collaboration Server disk capacity in megabytes. If the remaining disk capacity falls below this level an active alarm is raised. **Default:** 2048
MULTIPLE_SERVICES	Determines whether the Multiple Services option is be activated once the appropriate license is installed. Possible Values: YES / NO Default: NO

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
NUMERIC_CHAIR_PASS_DEFAULT_LEN	This flag enables or disables the automatic generation of chairperson passwords and determines the number of digits in the chairperson passwords assigned by the MCU. Possible values are: • **0** disables the automatic password generation. Any value other than 0 enables the automatic generation of chairperson passwords if the flag HIDE_CONFERENCE_PASSWORD is set to NO. • **1 – 16**, default: 6 (Standard Security Mode) If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_MAX_LEN	The maximum number of digits that the user can enter when manually assigning a password to the chairperson. Range: Default: 16
NUMERIC_CHAIR_PASS_MIN_LEN	Defines the minimum length required for the Chairperson password. Value: 0-16 Default:
NUMERIC_CONF_ID_LEN	Defines the number of digits in the Conference ID that will be assigned by the MCU. Enter 0 to disable the automatic assignment of IDs by the MCU and let the Collaboration Server user manually assign them. Range: 2-16 (Default: 4).
NUMERIC_CONF_ID_MAX_LEN	The maximum number of digits that the user can enter when manually assigning an ID to a conference. Range: 2-16 (Default: 8) **Note:** Selecting 2 limits the number of simultaneous ongoing conferences to 99.
NUMERIC_CONF_ID_MIN_LEN	The minimum number of digits that the user must enter when manually assigning an ID to a conference. Range: 2-16 (Default: 4) **Note:** Selecting 2 limits the number of simultaneous ongoing conferences to 99.

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
NUMERIC_CONF_PASS_DE FAULT_LEN	This flag enables or disables the automatic generation of conference passwords and determines the number of digits in the conference passwords assigned by the MCU. Possible values are: • **0** disables the automatic password generation. 　Any value other than 0 enables the automatic generation of conference passwords if the flag HIDE_CONFERENCE_PASSWORD is set to NO. • **1 – 16**, default: 6 If the default is used, in non-secured mode the system will automatically generate conference passwords that contain 6 characters.
NUMERIC_CONF_PASS_MA X_LEN	The maximum number of digits that the user can enter when manually assigning a password to the conference. Range: Default (both Modes): 16
NUMERIC_CONF_PASS_MI N_LEN	Defines the minimum length required for the Conference password. Value: 0-16 • Default:
PAL_NTSC_VIDEO_OUTPU T	When set to AUTO (default), the video output sent by the Collaboration Server is PAL. This ensures full synchronization between the frame rate of the speaker and the video encoder, ensuring smoother video. In environments where endpoints are PAL, the flag can be set accordingly to change the video encoding of the Collaboration Server to be compatible with the majority of endpoints in the call. Possible Value: PAL
RESTRICT_CONTENT_BRO ADCAST_TO_LECTURER	If set to YES, only the conference lecturer may send content to the conference. If set to NO, any conference participant can send content. Default: YES
RRQ_WITHOUT_GRQ	To enable registration, some gatekeepers require sending first RRQ and not GRQ. Set flag to **YES**, if this behavior is required by the gatekeeper in your environment. Default: NO. *GRQ (Gatekeeper Request)* - Gatekeeper discovery is the process an endpoint uses to determine which gatekeeper to register with. *RRQ* - registration request sent to the gatekeeper.

Table 20-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
SESSION_TIMEOUT_IN_MINUTES	If there is no input from the user or if the connection is idle for longer than the number of minutes specified by this flag, the connection to the Collaboration Server is terminated. Value: 0-999 0 - Session Timeout is disabled. Default: 0
SIP_AUTO_SUFFIX_EXTENSION	Used to automatically add a suffix to a SIP address (To Address) instead of adding it manually in the *Collaboration Server Web Client* (SIP address) when the SIP call is direct-dial and not through a Proxy. **Example:** Participant Name = john.smith Company Domain = maincorp.com SIP_AUTO_SUFFIX_EXTENSION flag value = @maincorp.com Entering john.smith will generate a SIP URI = john.smith@maincorp.com
STAR_DELIMITER_ALLOWED	When set to YES, an asterisk "*" can be used as a delimiter in Conference and Meeting Room dial strings. The dial string is first searched for "#' first followed by "*". Default: NO
TERMINATE_CONF_AFTER_CHAIR_DROPPED	From Version 8.1, this flag's functionality is replaced by the **Terminate Conference after Chairperson Drops** check box in the *Profile - IVR* dialog box. In versions prior to 8.1, if YES, sets conferences to automatically terminate if the Chairperson disconnects from the conference. This takes effect only if the *Conference Requires Chairperson* check box in the Conference Profile Properties, IVR Tab, is selected. Default: YES **Note:** In order for the "Chairperson Exit" message to be played this flag must be set to YES.

3   To modify a flag value, double-click or select the flag and click the **Edit Flag** button.

4   In the *New Value* field, enter the flag's new value.

5   Click **OK** to close the *Update Flag* dialog box.

6   Repeat steps 2–4 to modify additional flags.

7 Click **OK** to close the *System Flags* dialog box

> For flag changes (including deletion) to take effect, reset the MCU. For more information see "*Resetting the Collaboration Server (RMX)*" on page **19-54**.

Manually Adding and Deleting System Flags

To add a flag:

1 In the *System Flags* dialog box, click the **New Flag** (New Flag) button.

The *New Flag* dialog box is displayed.

```
New Flag                                    ☒

    New Flag:  [                              ]

    Value:     [                              ]

                        [   OK   ]  [  Cancel  ]
```
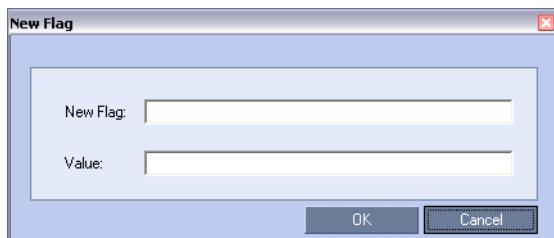
2 In the *New Flag* field enter the flag name.

3 In the *Value* field enter the flag value.

The following flags can be manually added to the *MCMS_PARAMETERS* tab:

Table 20-2 Manually Added System Flags – MCMS_PARAMETERS

Flag	Description
802_1X_CERTIFICATE_MODE	Not Supported in RMX 1800.
802_1X_SKIP_CERTIFICATE_VALIDATION	Not Supported in RMX 1800.
802_1X_CRL_MODE	Not Supported in RMX 1800.
802_FIPS_MODE	Not Supported in RMX 1800.
ACCEPT_VOIP_DTMF_TYPE	Defines the type of *DTMF* tones *(inband)* or digits *(outband)* that the Collaboration Server will accept in *VOIP* calls. **Range:** • **0** - Auto (default): *Inband* or *outband DTMF* tones/digits are accepted depending on the endpoint's current setting. If the endpoint switches from *inband* to *outband* or visa versa the value of the SET_DTMF_SOURCE_DIFF_IN_SEC flag determines the time interval after which both *inband* and *outband* tones/digits will be accepted. • **1** - *Outband* (H.245) only • **2** - *Inband* only

Table 20-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
ANAT_IP_PROTOCOL_SETTING	If YES, enables *Alternative Network Address Types*. For more information, see "*Alternative Network Address Types (ANAT)"* on page **23-49**. Range: DISABLED, AUTO, PREFER_IPv4, PREFER_IPv6 • Default: **YES**
APACHE_KEEP_ALIVE_TIMEOUT	If the connection is idle for longer than the number of seconds specified by this flag, the connection to the Collaboration Server is terminated. Value: 0 - 999 Default: 15 **Note:** A value of 0 results in an unlimited keep-alive duration.
AVOID_VIDEO_LOOP_BACK_IN_CASCADE	When set to YES the current speaker's image is not sent back through the participant link in cascaded conferences with conference layouts other than 1x1. Default: YES Range: YES / NO
BLOCK_CONTENT_LEGACY_FOR_LYNC	This flag is used to control the system behavior in an environment where some Lync clients use the Polycom CCS plug-in and some do not. When set to **NO** (default), Content is sent to all Lync clients over the video channel, including those with the plug-in installed, even when the *Send Content to Legacy Endpoints* is disabled. Other, non-Lync legacy endpoints will not be affected by this flag and will receive content according to the *Send Content to Legacy Endpoints* settings in the conference Profile. When set to **YES**, Content is not sent to Lync clients over the video channel including those with the Polycom CCS plug-in installed, even when the *Send Content to Legacy Endpoints* is enabled. Other, non-Lync legacy endpoints will not be affected by this flag and will receive content according to the *Send Content to Legacy Endpoints* settings in the conference Profile.
DETECT_SIP_EP_DISCONNECT _TIMER	The flag value indicates the amount of time in seconds to wait for an RTCP or RTP message to be received from the endpoint. When the time that was set in the system flag has elapsed and no RTCP or RTP audio or video message has been received on either the audio or the video channel, the MCU disconnects the SIP endpoint from the conference. Default: 20 (seconds) Range: 0 - 300 For more information see "*Detecting SIP Endpoint Disconnection"* on page **12-27**.

Table 20-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
DISABLE_DUMMY_REGIST RATION	Enables or disables SIP dummy registration on the domain. Possible Values: NO (Default) - Disables SIP dummy registration. YES - Enables SIP dummy registration. **Note:** For homologation and certification testing, the flag must be set to YES.
DTMF_FORWARD_ANY_DI GIT_TIMER_SECONDS	Used for DTMF code suppression in cascading conferences. Determines the time period (in seconds) that MCU A will forward DTMF inputs from conference A participants to MCU B. Flag range (in seconds): 0 - 360000 This flag is defined on MCU A (the calling MCU). For more information, see"*Video Layout in Cascading conferences (CP and mixed CP and SVC)"* on page **5-1**.
ENABLE_EPC	When set to YES (default), enables Polycom proprietary People+. When set to NO, disables this feature for all conferences and participants.
ENABLE_FLOW_CONTROL _REINVITE	Used to enable or disable sending a *re-INVITE* to endpoints to adjust their data rate. When set to YES, *re*-INVITE is used for endpoints that do not support *flow control* in SIP using either the *Information* or *RTCP Feedback* mechanisms. Default: NO.
ENABLE_H239	When set to YES, Content is sent via a separate Content channel. Endpoints that do not support H.239 Content sharing will not be able to receive When set to NO, the Content channel is closed. In such a case, H.239 Content is sent via the video channel ("people" video) enabling endpoints that do not support H.239 Content sharing to receive the Content in their video channel. Default: YES.
ENABLE_H239_ANNEX_T	In H.239-enabled MIH Cascading, when MGC is on level 1, enables sending Content using Annex T.
ENABLE_SELECTIVE_MIXI NG	Enables (default) or disables the Automatic muting of noisy AVC endpoints. For more details, see "*Permanent Conference"* on page **4-48**. When set to YES, the automatic muting of noisy endpoints can be enabled or disabled at the conference level in the *Conference Profile - Audio Settings* dialog box. When set to NO, the automatic muting of noisy endpoints is disabled at the conference level and cannot be enabled in the Conference *Profile - Audio Settings* dialog box. Default: YES **Note:** MCU reset is not required when changing the flag value.

Table 20-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
ENABLE_SIP_PEOPLE_PLUS_CONTENT	If security is of higher priority than SIP Content sharing, SIP People+Content can be disabled by setting this System Flag to NO. (The content management control (BFCP) utilizes an unsecured channel (60002/TCP) even when SIP TLS is enabled.) Default: YES
ENABLE_SIP_PPC_FOR_ALL_USER_AGENT	When set to YES, SIP People+Content and BFCP capabilities are declared with all vendors' endpoints. Default: YES Range: YES / NO
ENABLE_SIRENLPR	Enable / disable SirenLPR Audio Algorithm for use in IP (H.323, SIP) calls in both CP and VSW conferences. Range: YES / NO Default: YES
ENABLE_SIRENLPR_SIP_ENCRYPTION	Enables the *SirenLPR* audio algorithm when using encryption with the *SIP* protocol. Range: YES / NO Default: NO
ENABLE_VIDEO_PREVIEW	Enables the Video Preview feature. Default: YES. For more details, see "*Video Preview"* on page **4-21**.
FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION	When set to **YES**, the cascaded link is automatically set to Full Screen (1x1) in CP conferences forcing the speaker in one cascaded conference to display in full window in the video layout of the other conference. Set this flag to **NO** when connecting to an MGC using a cascaded link, if the MGC is functioning as a Gateway and participant layouts on the other network are not to be forced to 1X1. Default: YES
FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE	When set to **YES**, *Undefined participants* must connect encrypted, otherwise they are disconnected. When set to **NO** (default) and the conference *Encryption* in the *Profile* is set to "Encrypt When Possible", both Encrypted and Non-encrypted *Undefined participants* can connect to the same conferences, where encryption is the preferred setting. Default: NO
FORCE_G711A	Setting this flag forces the use of the *G711A Audio Codec.* **Possible values:** YES / NO **Default:** NO

Table 20-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
H239_FORCE_CAPABILITIES	When the flag is set to NO, the Collaboration Server only verifies that the endpoint supports the Content protocols: Up to H.264 or H.263. When set to YES, the Collaboration Server checks frame rate, resolution and all other parameters of the Content mode as declared by an endpoint before receiving or transmitting Content. Default: NO.
H264_HD_GRAPHICS_MIN_CONTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Graphics. Range: 0-1536 Default: 128
H264_HD_HIGHRES_MIN_CONTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Hi Resolution Graphics. Range: 0-1536 Default: 256
H264_HD_LIVEVIDEO_MIN_CONTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Live Video. Range: 0-1536 Default: 384
HIDE_CONFERENCE_PASSWORD	If set to YES: • Conference and Chairperson Passwords that are displayed in the *Collaboration Server Web Client* or *RMX Manager* are hidden when viewing the properties of the conference. • Automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags: 　• NUMERIC_CONF_PASS_DEFAULT _LEN 　• NUMERIC_CHAIR_PASS_ DEFAULT_LEN. For more information see "*Automatic Password Generation Flags"* on page **20-23** Default: NO.
IP_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the Polycom RMX 1800 from 1920Kbps to 18432, 100bits/sec to match the actual rate of the IP Only HD Video Switching conference running on the MGC. **Note:** If the flag MIX_LINK_ENVIRONMENT is set to NO, the *IP_ENVIRONMENT_LINK* flag must be set to YES.

Table 20-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
LAN_REDUNDANCY	Enables Local Area Network port redundancy. Default: NO Range: YES / NO Note: If the flag value is set to YES and either of the LAN connections (LAN1 or LAN2) experiences a problem, an active alarm is raised stating that there is no LAN connection, specifying both the card and port number.
MAX_TRACE_LEVEL	This flag indicates the debugging level for system support. **Possible values:** TRACE = t, DEBUG = d, INFO_NORMAL = n, INFO_HIGH = i, WARN = w, ERROR = e, FATAL = f, OFF = o. **Default:** n
MAXIMUM_RECORDING_LINKS	The maximum number of Recording Links available for selection in the Recording Links list and the Conference Profile - Recording dialog box. Range: 1 - 100 Default: 20
MINIMUM_FRAME_RATE_THRESHOLD_FOR_SD	Low quality, low frame rate video is prevented from being sent to endpoints by ensuring that an SD channel is not opened at frame rates below the specified value. Range: 0 -30 Default: 15
MIX_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the Polycom RMX 1800 from 1920Kbps to 17897, 100bits/sec to match the actual rate of the HD Video Switching conference running on the MGC. **Note:** If the flag MIX_LINK_ENVIRONMENT is set to YES, the IP_ENVIRONMENT_LINK flag must be set to NO.
NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT	Indicates how many times the Hello (keep alive) message is sent from the Collaboration Server to the endpoint in an environment that includes a Session Border Controller (SBC) with a 3-second interval between messages. Range: 1 to 10. Default:3
NUMBER_OF_REDIAL	Enter the number re dialing attempts required. Dialing may continue until the conference is terminated. Default: 3

Table 20-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
OCSP_RESPONDER_TIME OUT	Not Supported in RMX 1800. Determines the number of seconds the RMX is to wait for an OCSP response from the OCSP Responder before failing the connection. Network latency or slow WAN links can cause login problems when logging in to the RMX's Management Network.This System Flag's value determines the number of seconds the MCU is to wait for an OCSP response from the OCSP Responder before failing the connection. Default: 3 (seconds) Range: 1-20 (seconds)
PORT_GAUGE_ALARM	When set to YES, if system resource usage reaches the High Port Usage Threshold as defined for the Port Gauges, System Alerts in the form of an Active Alarm and an SNMP trap are generated.
PRESERVE_PARTY_CELL_ ON_FORCE_LAYOUT	Used to prevent reassignment of cells in a forced layout that were assigned to endpoints that have disconnected, paused their video, or have been removed from the conference. The cell will remain black until the endpoint reconnects or a new layout is used, or the conference ends. Range: YES / NO Default: NO • NO - Cells of dropped endpoints are reassigned. Endpoints that reconnect will be treated as new endpoints. • YES - Cells of dropped endpoints are not reassigned, but will be reserved until the endpoint reconnects. For information see the *Polycom RMX 1800 Getting Started Guide*, *""* on page **3-48**.
QOS_IP_AUDIO	Used to select the priority of audio packets when *DiffServ is* the is the selected method for packet priority encoding. Default: 0x31
QOS_IP_VIDEO	Used to select the priority of video packets when *DiffServ is* the is the selected method for packet priority encoding. Default: 0x31
QOS_MANAGEMENT_NET WORK	Enter the *DSCP* value for the *RMX Management Network*. Default: 0x10 Range: 0x00 - 0x3F
REDUCE_CAPS_FOR_RED COM_SIP	To accommodate Redcom's SDP size limit, when the flag value = YES, the SDP size is less than 2kb and includes only one audio and one video media line. Default: NO
REDIAL_INTERVAL_IN_SEC ONDS	Enter the number of seconds that the Collaboration Server should wait before successive re dialing attempts. Range: 0-30 (Default: 10)

Table 20-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
REDUCE_CAPS_FOR_RED COM_SIP	To accommodate Redcom's SDP size limit, when the flag value = YES, the SDP size is less than 2kb and includes only one audio and one video media line. Default: NO
REJECT_INCORRECT_PRE CEDENCE_DOMAIN_NAME	When set to YES, when the Precedence Domain of a SIP dial-in call does not match the Precedence Domain of the RMX, the call is rejected. For more information, see "*MLPP (Multi Level Precedence and Preemption)*" on page **23-36**. Possible values: YES/NO Default: No
REMOVE_H323_EPC_CAP_ TO_NON_POLYCOM_VEND OR	Used to disable *EPC* protocol. Use of *Polycom's* proprietary protocol, *High Profile*, *EPC*, may result in interoperability issues when used with other vendors' endpoints. **Possible values:** YES / NO **Default:** NO
REMOVE_H323_HIGH_PRO FILE_CAP_TO_NON_POLY COM_VENDOR	Used to disable *High Profile* protocol. Use of *Polycom's* proprietary protocol, *High Profile*, may result in interoperability issues when used with other vendors' endpoints. **Possible values:** YES / NO **Default:** NO
REMOVE_H323_HIGH_QUA LITY_AUDIO_CAP_TO_NON _POLYCOM_VENDOR	Used to disable the following *Audio Codecs*: • G7221C • G7221 • Siren22 • Siren14 **Possible values:** YES / NO **Default:** NO
REMOVE_H323_LPR_CAP_ TO_NON_POLYCOM_VEND OR	Used to disable *H.323 LPR* protocol. Use of *Polycom's* proprietary protocol, *H.323 LPR*, may result in interoperability issues when used with other vendors' endpoints. **Possible values:** YES / NO **Default:** NO
REMOVE_IP_IF_NUMBER_ EXISTS	Between the time a conference is scheduled and when it becomes active, the IP of an endpoint may change, especially in an environment that uses DHCP. This flag determines if the *E.164* number is to be substituted for the IP address in the dial string. Range: YES / NO Default: YES - The IP address will be substituted with the E.164 number.
RMX_MANAGEMENT_SEC URITY_PROTOCOL	Enter the protocol to be used for secure communications. **Default: TLSV1_SSLV3 (both).**

Table 20-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
RTCP_FIR_ENABLE	When set to YES, the *Full Intra Request* (*FIR*) is sent as *INFO* (and not *RTCP*). Default = YES
RTCP_FLOW_CONTROL_T MMBR_ENABLE	Enables/disables the SIP RTCP flow control parameter. Default: YES
RTCP_FLOW_CONTROL_T MMBR_INTERVAL	Modifies the interval (in seconds) of the TMMBR (Temporary Maximum Media Stream Bit Rate) parameter for SIP RTCP flow control. Range: 5 - 999 (seconds) Default: 180
RTCP_PLI_ENABLE	When set to YES, the (Picture Loss Indication (*PLI*) is sent as *INFO* (and not *RTCP*). Default = YES
RTCP_QOS_IS_EQUAL_TO _RTP	Range: YES/NO Default: YES
SEND_SIP_BUSY_UPON_R ESOURCE_THRESHOLD	When set to **YES**, it enables the Collaboration Server to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the Collaboration Server whose audio resource usage exceeded the Port Usage threshold. When set to **NO**, the system does limit the SIP audio endpoint connections to a certain capacity and will not send a busy notification when the resource capacity threshold is exceeded. Default: NO
SET_DTMF_SOURCE_DIFF _IN_SEC	If the ACCEPT_VOIP_DTMF_TYPE flag is set to 0 (Auto) this flag determines the interval, in seconds after which the Collaboration Server will accept both *DTMF* tones *(inband)* and digits *(outband)*. **Default:** 120

Table 20-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
SIP_BFCP_DIAL_OUT_MODE	Controls *BFCP's* use of *UDP* and *TCP* protocols for dial-out *SIP Client* connections according to its value: • **AUTO** (Default) *If SIP Client* supports *UDP, TCP* or *UDP* and *TCP*: - BFCP/UDP is selected as *Content* sharing protocol. • **UDP** *If SIP Client* supports *UDP* or UDP and TCP: - *BFCP/UDP* selected as *Content* sharing protocol. *If SIP Client* supports *TCP* - Cannot share *Content*. • **TCP** *If SIP Client* supports *TCP* or *UDP* and *TCP* - BFCP/TCP selected as Content sharing protocol. *If SIP Client* supports UDP - Cannot share Content.
SIP_ENABLE_FECC	By default, FECC support for SIP endpoints is enabled at the MCU level. You can disable it by manually adding this flag and setting it to NO.
SIP_TCP_PORT_ADDR_STRATEGY	Setting the flag to 1 prevents the use of two sockets for one SIP call - one for inbound traffic, one for outbound traffic. This is done by inserting port "5060/5061" into the Route[0] header. **Possible values:** • 0 - Inbound traffic on port 5060/5061 outbound traffic on port 60000 • 1 - Both inbound and outbound traffic on port 5060/5061 **Default**: 1
SUPPORT_HIGH _PROFILE	Enables or disables the support of *High Profile* video protocol in CP conferences. This flag is specific to CP conferences and has no effect on VSW conferences. Range: YES / NO Default: YES
TCP_RETRANSMISSION_TIMEOUT	The number of seconds the server will wait for a *TCP* client to answer a call before closing the connection. Default = 5 (seconds)
V35_MULTIPLE_SERVICES	Not Supported in RMX 1800. If the connection of multiple Serial Gateways to RTM-LAN cards is required: The V35_MULTIPLE_SERVICES System Flag must be set to YES. The default value of the V35_MULTIPLE_SERVICES System Flag is NO, enabling only one Serial Gateway to be supported per RTM-LAN card.

Table 20-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
WRONG_NUMBER_DIAL_RETRIES	The number of re-dial attempts for a wrong destination number or a wrong destination number time-out. Range: 0 - 5 Default: 3 A flag value of 0 means that no redials are attempted.

4 Click **OK** to close the *New Flag* dialog box.
The new flag is added to the flags list.

5 Click **OK** to close the *System Flags* dialog box.

> For flag changes (including deletion) to take effect, reset the MCU. For more information see "*Resetting the Collaboration Server (RMX)"* on page **19-54**.

Manually Adding Flags to the CS_MODULE_PARAMETERS Tab

Using the procedure to manually add flags to the System Configuration, the following flags can be manually added to the **CS_MODULE_PARAMETERS** tab:

Table 20-3 Manually Added Flags - CS_MODULE_PARAMETERS Tab

Flag	Description
H323_TIMERS_SET_INDEX	Enables or disables H.323 index timer according to standard or proprietary H.323 protocol. Possible values: 0 (Default) - Sets the H.323 index timer to Polycom proprietary. 1 - Sets the H.323 index timer based on the H.323 Standard recommendation. **Note:** For homologation and certification testing, this flag must be set to 1.
QOS_IP_SIGNALING	Used to select the priority of IP packets when *DiffServ is* the is the selected method for packet priority encoding. Range: 0x## Default: 0x28
SIP_TIMERS_SET_INDEX	SIP Timer type timeout settings according to standard or proprietary protocol. Possible values are: 0 - Default 1 - SIP Standard recommendation. **Note:** For homologation and certification testing, this flag must be set to 1.

Deleting a Flag

To delete a flag:

1 In the *System Flags* dialog box, select the flag to delete and click the **Delete Flag** button.

2 In the confirmation message box, click **Yes** to confirm.

3 Click **OK to** close the *System Flags* dialog box.

Auto Layout Configuration

The *Auto Layout* option lets the Collaboration Server automatically select the conference video layout based on the number of participants currently connected to the conference. You can modify the default selection of the conference video layout to customize it to your conferencing preferences.

Customizing the Default Auto Layout

The default *Auto Layout* is controlled by 13 flags:

PREDEFINED_AUTO_LAYOUT_0, … , **PREDEFINED_AUTO_LAYOUT_12**

Each of the 11 *Auto Layout* flags can be left at its default value, or set to any of the *Possible Values* listed in Table 20-4.
The flag that controls the *Auto Layout* you wish to modify must be added to the *System Configuration* file. For more information see "*Modifying System Flags"* on page **20-1**.

Table 20-4 Flags: PREDEFINED_AUTO_LAYOUT_0,...,10

Flag Name: PREDEFINED_AUTO_LAYOUT_n (n = Number of Participants)		
n	**Default Value**	**Possible Values**
0	CP_LAYOUT_1X1	CP_LAYOUT_1X1
1	CP_LAYOUT_1X1	CP_LAYOUT_1X2
2	CP_LAYOUT_1X1	CP_LAYOUT_1X2HOR
3	CP_LAYOUT_1x2VER	CP_LAYOUT_1X2VER
4	CP_LAYOUT_2X2	CP_LAYOUT_2X1
5	CP_LAYOUT_2X2	CP_LAYOUT_1P2HOR
6	CP_LAYOUT_1P5	CP_LAYOUT_1P2HOR_UP
7	CP_LAYOUT_1P5	CP_LAYOUT_1P2VER
8	CP_LAYOUT_1P7	CP_LAYOUT_2X2
9	CP_LAYOUT_1P7	CP_LAYOUT_1P3HOR_UP
10	CP_LAYOUT_1P7	CP_LAYOUT_1P3VER
11	CP_LAYOUT_2P8	CP_LAYOUT_1P4HOR
12	CP_LAYOUT_1P12	CP_LAYOUT_1P4HOR_UP

Table 20-4 Flags: PREDEFINED_AUTO_LAYOUT_0,...,10 (Continued)

Flag Name: PREDEFINED_AUTO_LAYOUT_n (n = Number of Participants)		
n	**Default Value**	**Possible Values**
		CP_LAYOUT_1P4VER
		CP_LAYOUT_1P5
		CP_LAYOUT_1P7
		CP_LAYOUT_1P8UP
		CP_LAYOUT_1P8CENT
		CP_LAYOUT_1P8HOR_UP
		CP_LAYOUT_3X3
		CP_LAYOUT_2P8
		CP_LAYOUT_1P12
		CP_LAYOUT_4X4

Example:

Table 20-5 illustrates the effect of modifying the **PREDEFINED_AUTO_LAYOUT_5** flag in conferences with fewer or more participants than the number of windows selected in the default layout.

Table 20-5 Example: Modifying PREDEFINED_AUTO_LAYOUT_5 Flag

Flag	Set to Possible Value	Number of Participants	Participant's View
PREDEFINED _AUTO_LAYOUT_5 *Default =*	CP_LAYOUT _1x2VER 	3	Voice activated switching displays the current speaker in the left window of the video layout and only the two last speakers are displayed.
		7	
	CP_LAYOUT _1P5 	3	Voice activated switching displays the current speaker in the large (top left) window of the video layout.
		7	Voice activated switching displays the current speaker in the top left window of the video layout.
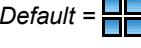
Automatic Password Generation Flags

The Collaboration Server can be configured to automatically generate conference and chairperson passwords when the *Conference Password* and *Chairperson Password* fields are left blank.

Guidelines

- If the flag **HIDE_CONFERENCE_PASSWORD** is set to **YES**, the automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags NUMERIC_CONF_PASS_DEFAULT_LEN and NUMERIC_CHAIR_PASS_ DEFAULT _LEN.

- The automatic generation of conference passwords is enabled/disabled by the flag NUMERIC_CONF_PASS_DEFAULT_LEN.

- The automatic generation of chairperson passwords is enabled/disabled by the flag NUMERIC_CHAIR_PASS_ DEFAULT _LEN.
- The automatically generated passwords will be numeric and random.
- The passwords are automatically assigned to ongoing conferences, Meeting Rooms and Reservations at the end of the creation process (once they are added to the Collaboration Server).
- Automatically assigned passwords can be manually changed through the *Conference/Meeting Room/Reservation Properties* dialog boxes.
- Deleting an automatically created password will not cause the system to generate a new password and the new password must be added manually or the field can be left blank.
- If a password was assigned to the conference via Microsoft Outlook using the PCO add-in, the system does not change these passwords and additional passwords will not be generated (for example, if only the conference password was assigned a chairperson password will not be assigned).
- If the flag values (i.e. the password lengths) are changed, passwords that were already assigned to conferences, Meeting Rooms and Reservations will not change and they can be activated using the existing passwords. Only new conferencing entities will be affected by the change.

> Do not enable this option in an environment that includes a *Polycom DMA* system.

Enabling the Automatic Generation of Passwords

To enable the automatic generation of passwords, the following flags have to be defined:

Table 20-6 Automatic Password Generation Flags

Flag	Description
HIDE_CONFERENCE_PASSWORD	**NO (default)** - Conference and chairperson passwords are displayed when viewing the Conference/Meeting Room/ Reservation properties. It also enables the automatic generation of passwords in general. **Yes** - Conference and Chairperson Passwords are hidden (they are replaced by asterisks). It also disables the automatic generation of passwords.
NUMERIC_CONF_PASS_MIN_LEN	Enter the minimum number of characters required for conference passwords. Possible values: **0 – 16**. **0 (default)** means no minimum length.
NUMERIC_CHAIR_PASS_MIN_LEN	Enter the minimum number of characters required for chairperson passwords. Possible values: **0 – 16**. **0 (default)** means no minimum length. However this setting cannot be applied when the Collaboration Server is in *Ultra Secure Mode*.

Table 20-6 *Automatic Password Generation Flags (Continued)*

Flag	Description
NUMERIC_CONF_PASS_MAX_LEN	Enter the maximum number of characters permitted for conference passwords. Possible values: **0 – 16** **16 (default)** - Conference password maximum length is 16 characters.
NUMERIC_CHAIR_PASS_MAX_LEN	Enter the maximum number of characters permitted for chairperson passwords. Possible values: **0 – 16** **16 (default)** - chairperson password maximum length is 16 characters.
NUMERIC_CONF_PASS_DEFAULT_LEN	This flag enables or disables the automatic generation of conference passwords. The length of the automatically generated passwords is determined by the flag value. Possible values: Enter **0** to disable the automatic generation of passwords. Any value other than 0 enables the automatic generation of conference passwords provided the flag *HIDE_CONFERENCE_PASSWORD is set to NO.* If the default is used, in non-secured mode the system will automatically generate conference passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_ DEFAULT_LEN	This flag enables or disables the automatic generation of chairperson passwords. The length of the automatically generated passwords is determined by the flag value. Possible values: Enter **0** to disable the automatic generation of passwords. Any value other than 0 enables the automatic generation of chairperson passwords provided the flag *HIDE_CONFERENCE_PASSWORD is set to NO.* If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.

If the default password length defined by the NUMERIC_CONF_PASS_DEFAULT_LEN or NUMERIC_CHAIR_PASS_ DEFAULT LEN does not fall within the range defined by the minimum and maximum length an appropriate fault is added to the Faults list.

Collaboration Server Hardware Monitoring

The status and properties of the Collaboration Server hardware components can be viewed in the *Hardware Monitor* list pane.

Viewing the Status of the Hardware Components

The *Hardware Monitor's* status column displays the present status of the hardware components. In addition to the status, temperature and voltage indications are provided for each component.

To view the status of the hardware components on the RMX 1800:

>> In the *RMX Management* pane, click the **Hardware Monitor** button.

The *Hardware Monitor* pane is displayed.

Slot	Type	Status	Temperature	Voltage
	RMX	Normal	Normal	Normal
1	DSP Card	Normal	Normal	-
2	DSP Card	Normal	Normal	-
3	DSP Card	Normal	Normal	-
	FANS	Normal	-	-
	PWR	Normal	-	Normal
	LANS	Normal	-	-

The *Hardware Monitor* pane displays the following Collaboration Server hardware component's status columns:

Table 21-1   Hardware Monitor Pane Status Columns

Field	Description
Slot	Displays an icon according to the Hardware component type and the slot number. The icon displays the hardware status as follows: • An exclamation point (**!**) indicates errors in the hardware component. • Card icon with the reset button (🖥) indicates that the hardware component is currently resetting.
Type	The type of hardware component card.

Table 21-1   Hardware Monitor Pane Status Columns (Continued)

Field	Description
Status	The current status of the hardware component; *Normal, Major, Critical, Resetting, Diagnostics, or Empty.*
Temperature	Monitors the temperature of the hardware components; Normal, Major and Critical. **Note:** Critical condition invokes a system shut down.
Voltage	The voltage threshold of the hardware component; either *Normal* or *Major*.

Hardware Monitor Pane Tool bar

The following buttons appear in the tool bar of the Hardware Monitor:

Table 21-2   Hardware Monitor Pane Tool Bar Buttons

Button	Name	Description
	System Reset	Resets and restarts the system. Resetting saves settings and information that you changed in the system, i.e. IP Services, etc...
	System Shut Down	Shuts down the system into a standby mode. When the user in the *RMX Manager/Client* presses the *System Shut Down* (red) button in the H*ardware Monitor* tool bar, the system should enter a standby mode and the LED turns ON. Turn the system OFF/ON to exit the standby mode.
	Active Diagnostic Mode	Activates Diagnostic mode. The system restarts and enter the Diagnostic mode and you can perform tests to detect malfunctions in the hardware component's performance. **Note**: Only Polycom Support can perform Diagnostic tests. For more information, contact your Polycom Support.

Viewing the Properties of RMX 1800 Hardware Components

The properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

*   MCU Properties (RMX 1800)
*   Card Properties (DSP cards)
*   Supporting Hardware Components Properties (FANS, LAN, PWR)

No properties are provided for Power Supply (PWR). For more information, see the *RMX 1800 Hardware Guide,* "*RealPresence Collaboration Server 1800 Specifications"* on page 2.

To view the MCU properties:

1   In the *Hardware Monitor* pane, either double-click or right-click and select **Properties** for *Polycom RMX 1800, slot 0*.

The following information is displayed:

Field	Description
Hardware Version	The version of the server hardware.
Firmware Version	The version of the BIOS installed on the server.
Serial Number	The serial number of the server hardware.
Card Type	Displays the type of card that occupies the slot.
Card Part Number	The part number of this card.
Card MAC Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second MAC address.

2 Click the *Active Alarms* tab to view alarms related to the Collaboration Server, i.e. temperatures and main power sensors.

The *Active Alarms* dialog box displays fields that relate to faults and errors detected on the Collaboration Server by sensors. The *Active Alarm*s dialog box is divided into two sections: *hardware Alarm List* and *SW Alarm List*.

Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm: Critical (RED), Major (ORANGE) and Normal (GREEN).

To view the card properties:

1 In the *Hardware Monitor* pane, right-click and select **properties** for the desired card.
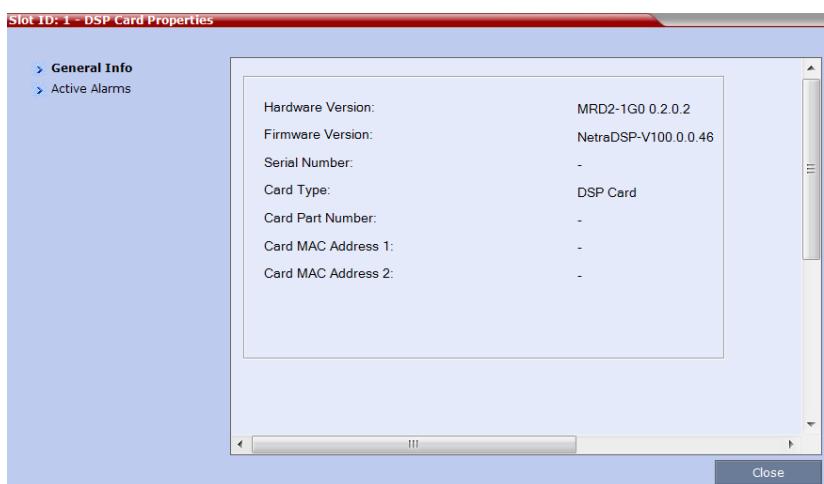
The mapping between the DSP slot IDs and the physical PCI slots is as the following:
- Slot ID 1: Riser PCI slot 0 (in the middle)
- Slot ID 2: Riser PCI slot 1 (bottom)
- Slot ID 3: Riser PCI slot 2 (top)

The following information is displayed:

Table 21-3 *Card Properties - General Info*

Field	Description
Hardware Version	The hardware component's version number.
Firmware Version	The version number of the software installed on card.
Serial Number	The hardware component's serial number.
Card Type	Displays the type of card that occupies the slot.
Card Part Number	The part number of the hardware component's board.
Card Mac Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second MAC address.

2 Click the **Active Alarms** tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.

For more information, see "*Active Alarms*" on page **21-5**.

3 Click **Close** to return to the *Hardware Monitor* pane.

To view the resource usage on a DSP card:

1 In the *Hardware Monitor* pane, double-click a desired DSP card.

2 The available chip list opens. You can find the following information:

Field	Description
Type	Media type this chip is used for processing.
Configuration	
Occupied	Whether this chip is used.
Faulty	Whether this chip functions properly.
Disabled	Whether this chip is disabled.
Location	
Network Service	Which network service this chip is associated with.
Percentage Occupied	The percentage of the resource used on this chip.

3 To view the port usage of a specific chip, double-click the desired chip.

You can find the following information:

Field	Description
Port ID	The ID of the port.
Active	Whether this port is active.

Field	Description
Percentage Occupied	The percentage of the resource used on this chip.
Port Type	The type of this port.

To view the supporting hardware components properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the *General Info* tab displayed.

FAN Properties:

The Collaboration Server unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.
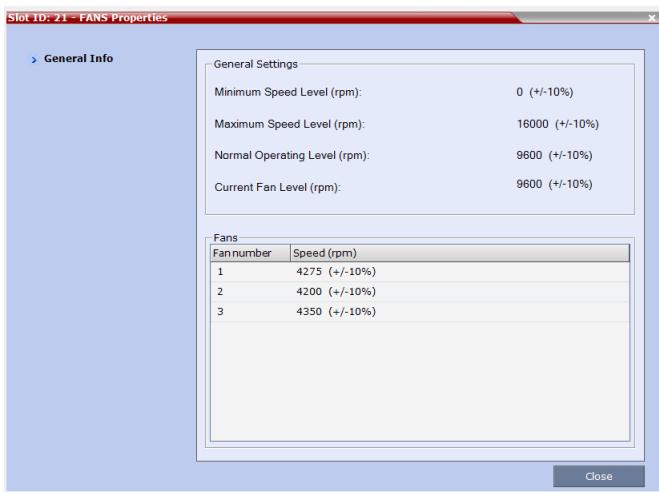
Table 21-4 FANS Properties - General Info

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Current Fan Level (rpm)	The current operating level of the fans.
Fans	
Fan 1 Speed (rpm)	Present speed of fan 1.
Fan 2 Speed (rpm)	Present speed of fan 2.
Fan 3 Speed (rpm)	Present speed of fan 3.

LAN 1 and LAN 2, Properties:

The Collaboration Server unit's chassis contains two external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peak detector to log the maximal values, since the last peak values reset.
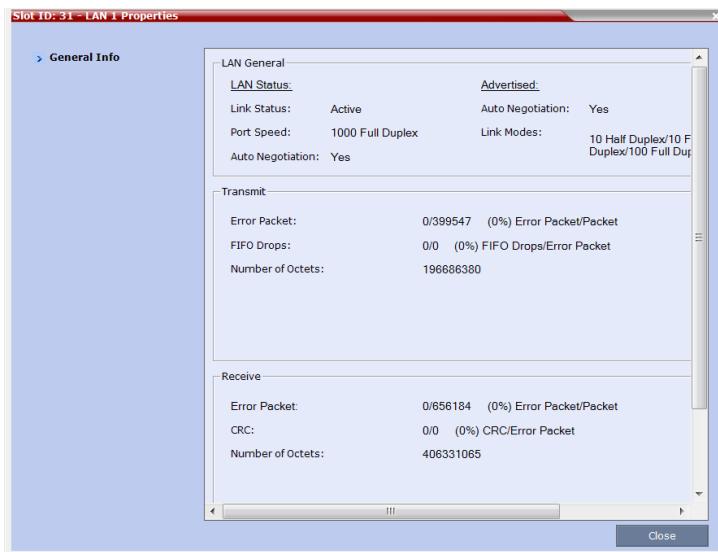
2 Click **Close** to return to the *Hardware Monitor* pane.

Resetting the RMX 1800 DSP cards

If the DSP cards don't function properly, you can reset them during a meeting.

When you reset a DSP card during a meeting, the system switches the impacted meeting media to other DSP cards, if available. If no other DSP cards available, the impacted meeting media is lost and there may be few seconds' pause in the meeting video.

Only Polycom Support can test DSP cards. For more information, contact your Polycom Support.

To reset a DSP card:

1 In the *RMX Management* pane, click the **Hardware Monitor** button.

The *Hardware Monitor* pane appears.

2 Right-click a desired DSP card and select **Rescue**.

3   When asked "Are you sure you want to send the rescue command to the card?", click **Yes**.

The card resets and its **Status** changes to **Resetting**. Upon the completion of the reset, its **Status** changes back to **Normal**.

Temperature Thresholds

On each Collaboration Server card or there are temperature sensors that are placed near specific components on the card. In the *Hardware Monitor* you can view the properties of each card together with their temperature statuses. By right clicking on any card and viewing the cards *Properties*, the A*ctive Alarms* tab displays all the card sensors, their statuses and lists each sensor's temperature specifications. When the temperature on the cards initially rises, a fault could be triggered and can viewed in the *System Alerts, Faults List*. Load issues can arise when the system nears the maximum conference mark or high port capacity occurs on an Collaboration Server resulting in *Upper Major* or *Upper Critical* faults.

> With an Upper Major alarm activation it is recommended to perform the following checks: Fans/fan tray functions, Overall System Ventilation and Filter (top, bottom & sides free and no dust) and Room temperature (cool). When no apparent cause can be found, then contact your next level of support.

However, only when the *Upper Critical* threshold is passed does the Collaboration Server system as a precaution initiate a system shutdown.

Slot	Type	Status	Temperature	Voltage
	RMX	Normal	Normal	Normal
	FANS	Normal	Normal	Normal
	PWR	Normal	-	Normal
	LANS	Normal	-	-

Figure 21-1 RMX 1800 Hardware Monitor pane

Appendix A

Disconnection Causes

If a participant was unable to connect to a conference or was disconnected from a conference, the **Connection Status** tab in the *Participant Properties* dialog box indicates the call disconnection cause. In some cases, a possible solution may be displayed.

A video participant who is unable to connect the video channels, but is able to connect as an audio only participant, is referred to as a Secondary participant. For Secondary participants, the **Connection Status** tab in the *Participant Properties* dialog box indicates the video disconnection cause. In some cases, a possible solution may be indicated.

The table below lists the call disconnection causes that can be displayed in the Call Disconnection Cause field and provides an explanation of each message

IP Disconnection Causes

Table A-1   Call Disconnection Causes

Disconnection Cause	Description
Disconnected by User	The user disconnected the endpoint from the conference.
Remote device did not open the encryption signaling channel	The endpoint did not open the encryption signaling channel.
Remote devices selected encryption algorithm does not match the local selected encryption algorithm	The encryption algorithm selected by the endpoint does not match the MCU's encryption algorithm.
Resources deficiency	Insufficient resources available.
Call close. Call closed by MCU	The MCU disconnected the call.
H323 call close. No port left for audio	Insufficient audio ports.
H323 call close. No port left for video	The required video ports exceed the number of ports allocated to video in fixed ports.
H323 call close. No port left for FECC	The required data ports exceed the number of ports allocated to data in fixed ports.
H323 call close. No control port left	The required control ports exceed the number of ports allocated to control data in fixed ports.
H323 call close. No port left for videocont	The required video content ports exceed the number of ports allocated to video content in fixed ports.

Table A-1   *Call Disconnection Causes (Continued)*

Disconnection Cause	Description
H323 call closed. Small bandwidth	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. No port left	There are no free ports left in the IP card.
Caller not registered	The calling endpoint is not registered in the gatekeeper.
H323 call closed. ARQ timeout	The endpoint sent an ARQ message to the gatekeeper, but the gatekeeper did not respond before timeout.
H323 call closed. DRQ timeout	The endpoint sent a DRQ message to the gatekeeper, but the gatekeeper did not respond before timeout.
H323 call closed. Alt Gatekeeper failure	An alternate gatekeeper failure occurred.
H323 call closed. Gatekeeper failure	A gatekeeper failure occurred.
H323 call closed. Remote busy	The endpoint was busy. (Applicable only to dial-out)
H323 call closed. Normal	The call ended normally, for example, the endpoint disconnected.
H323 call closed. Remote reject	The endpoint rejected the call.
H323 call closed. Remote unreachable	The call remained idle for more than 30 seconds and was disconnected because the destination device did not answer. Possible causes can be due to network problems, the gatekeeper could not find the endpoint's address, or the endpoint was busy or unavailable (for example, the "do not disturb" status is selected).
H323 call closed. Unknown reason	The reason for the disconnection is unknown, for example, the endpoint disconnected without giving a reason.
H323 call closed. Faulty destination address	Incorrect address format.
H323 call closed. Small bandwidth	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. Gatekeeper reject ARQ	The gatekeeper rejected the endpoint's ARQ.
H323 call closed. No port left	There are no ports left in the IP card.
H323 call closed. Gatekeeper DRQ	The gatekeeper sent a DRQ.
H323 call closed. No destination IP address	For internal use.
H323 call. Call failed prior or during the capabilities negotiation stage	The endpoint did not send its capabilities to the gatekeeper.
H323 call closed. Audio channels didn't open before timeout	The endpoint did not open the audio channel.

Table A-1   *Call Disconnection Causes (Continued)*

Disconnection Cause	Description
H323 call closed. Remote sent bad capability	There was a problem in the capabilities sent by the endpoint.
H323 call closed. Local capability wasn't accepted by remote	The endpoint did not accept the capabilities sent by the gatekeeper.
H323 failure	Internal error occurred.
H323 call closed. Remote stop responding	The endpoint stopped responding.
H323 call closed. Master slave problem	A People + Content cascading failure occurred.
SIP bad name	The conference name is incompatible with SIP standards.
SIP bad status	A general IP card error occurred.
SIP busy everywhere	The participant's endpoints were contacted successfully, but the participant is busy and does not wish to take the call at this time.
SIP busy here	The participant's endpoint was contacted successfully, but the participant is currently not willing or able to take additional calls.
SIP capabilities don't match	The remote device capabilities are not compatible with the conference settings.
SIP card rejected channels	The IP card could not open the media channels.
SIP client error 400	The endpoint sent a SIP Client Error 400 (Bad Request) response. The request could not be understood due to malformed syntax.
SIP client error 402	The endpoint sent a SIP Client Error 402 (Payment Required) response.
SIP client error 405	The endpoint sent a SIP Client Error 405 (Method Not Allowed) response. The method specified in the Request-Line is understood, but not allowed for the address identified by the Request-URI.
SIP client error 406	The endpoint sent a SIP Client Error 406 (Not Acceptable) resources. The remote endpoint cannot accept the call because it does not have the necessary responses. The resource identified by the request is only capable of generating response entities that have content characteristics not acceptable according to the Accept header field sent in the request.

Table A-1   *Call Disconnection Causes (Continued)*

Disconnection Cause	Description
SIP client error 407	The endpoint sent a SIP Client Error 407 (Proxy Authentication Required) response. The client must first authenticate itself with the proxy.
SIP client error 409	The endpoint sent a SIP Client Error 409 (Conflict) response. The request could not be completed due to a conflict with the current state of the resource.
SIP client error 411	The endpoint sent a SIP Client Error 411 (Length Required) response. The server refuses to accept the request without a defined Content Length.
SIP client error 413	The endpoint sent a SIP Client Error 413 (Request Entity Too Large) response. The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
SIP client error 414	The endpoint sent a SIP Client Error 414 (Request-URI Too Long) response. The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
SIP client error 420	The endpoint sent a SIP Client Error 420 (Bad Extension) response. The server did not understand the protocol extension specified in a Require header field.
SIP client error 481	The endpoint sent a SIP Client Error 481 (Call/Transaction Does Not Exist) response.
SIP client error 482	The endpoint sent a SIP Client Error 482 (Loop Detected) response.
SIP client error 483	The endpoint sent a SIP Client Error 483 (Too Many Hops) response.
SIP client error 484	The endpoint sent a SIP Client Error 484 (Address Incomplete) response. The server received a request with a To address or Request-URI that was incomplete.
SIP client error 485	The endpoint sent a SIP Client Error 485 (Ambiguous) response. The address provided in the request (Request-URI) was ambiguous.
SIP client error 488	The endpoint sent a SIP Client Error 488 (Not Acceptable Here) response.

Table A-1 *Call Disconnection Causes (Continued)*

Disconnection Cause	Description
SIP forbidden	The SIP server rejected the request. The server understood the request, but is refusing to fulfill it.
SIP global failure 603	A SIP Global Failure 603 (Decline) response was returned. The participant's endpoint was successfully contacted, but the participant explicitly does not wish to or cannot participate.
SIP global failure 604	A SIP Global Failure 604 (Does Not Exist Anywhere) response was returned. The server has authoritative information that the user indicated in the Request-URI does not exist anywhere.
SIP global failure 606	A SIP Global Failure 606 (Not Acceptable) response was returned.
SIP gone	The requested resource is no longer available at the Server and no forwarding address is known.
SIP moved permanently	The endpoint moved permanently. The user can no longer be found at the address in the Request-URI.
SIP moved temporarily	The remote endpoint moved temporarily.
SIP not found	The endpoint was not found. The server has definitive information that the user does not exist at the domain specified in the Request-URI.
SIP redirection 300	A SIP Redirection 300 (Multiple Choices) response was returned.
SIP redirection 305	A SIP Redirection 305 (Use Proxy) response was returned. The requested resource MUST be accessed through the proxy given by the Contact field.
SIP redirection 380	A SIP Redirection 380 (Alternative Service) response was returned. The call was not successful, but alternative services are possible.
SIP remote cancelled call	The endpoint canceled the call.
SIP remote closed call	The endpoint ended the call.
SIP remote stopped responding	The endpoint is not responding.
SIP remote unreachable	The endpoint could not be reached.
SIP request terminated	The endpoint terminated the request. The request was terminated by a BYE or CANCEL request.
SIP request timeout	The request was timed out.

Table A-1   *Call Disconnection Causes (Continued)*

Disconnection Cause	Description
SIP server error 500	The SIP server sent a SIP Server Error 500 (Server Internal Error) response. The server encountered an unexpected condition that prevented it from fulfilling the request.
SIP server error 501	The SIP server sent a SIP Server Error 501 (Not Implemented) response. The server does not support the functionality required to fulfill the request.
SIP server error 502	The SIP server sent a SIP Server Error 502 (Bad Gateway) response. The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
SIP server error 503	The SIP server sent a SIP Server Error 503 (Service Unavailable) response. The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.
SIP server error 504	The SIP server sent a SIP Server Error 504 (Server Time-out) response. The server did not receive a timely response from an external server it accessed in attempting to process the request.
SIP server error 505	The SIP server sent a SIP Server Error 505 (Version Not Supported) response. The server does not support, or refuses to support, the SIP protocol version that was used in the request.
SIP temporarily not available	The participant's endpoint was contacted successfully but the participant is currently unavailable (e.g., not logged in or logged in such a manner as to preclude communication with the participant).
SIP remote device did not respond in the given time frame	The endpoint did not respond in the given time frame.
SIP trans error TCP Invite	A SIP Invite was sent via TCP, but the endpoint was not found.
SIP transport error	Unable to initiate connection with the endpoint.
SIP unauthorized	The request requires user authentication.
SIP unsupported media type	The server is refusing to service the request because the message body of the request is in a format not supported by the requested resource for the requested method.

Appendix B

Active Alarms

Alarm Code	Alarm Description
A matching activation key is required. To cancel the upgrade process, reset the Collaboration Server	The system upgrade requires that a valid activation key be entered. If none is available, resetting the Collaboration Server will cancel the upgrade and return the Collaboration Server to the previous version.
A new activation key was loaded. Reset the system.	A new activation key was loaded: Reset the MCU.
A new version was installed. Reset the system.	A new version was installed: Reset the MCU.
Alarm generated by a Central Signaling component	A system alert was generated by a component of the Central Signaling.
Alarm generated by an internal component	A system alert was generated by an internal system component.
Allocation mode was modified	
Automatic reset is unavailable in Safe Mode	The system switches to safe mode if many resets occur during startup. To prevent additional resets, and allow the system to complete the startup process the automatic system resets are blocked.
Backup of audit files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that audit files need to be backed up.
Backup of CDR files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that CDR files need to be backed up.
Backup of log files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that log files need to be backed up.
Card configuration event	
Cards wrong file's mode	

Table B-1 *Active Alarms (Continued)*

Alarm Code	Alarm Description
Central signaling component failure	Possible explanations: • Central signaling component failure; unit type: [NonComponent\CSMngnt\CSH323\CSSIP] • Central signaling component failure; unit type: (invalid: [NonComponent\CSMngnt\CSH323\CSSIP]) • Central signaling component failure - Invalid failure type. Unit id: [id], Type: [NonComponent\CSMngnt\CSH323\CSSIP], Status: [Ok\Failed\Recovered] • Central signaling component failure - Invalid failure type
Central Signaling indicating Faulty status	Central signaling failure detected in IP Network Service.
Central Signaling indicating Recovery status	
Central Signaling startup failure	Central Signaling component is down.
Conference Encryption Error	
Configuration of external database did not complete.	Check the configuration of the external DB.
CPU IPMC software was not updated.	Turn off the MCU and then turn it on.
CPU slot ID not identified	The CPU slot ID required for Ethernet Settings was not provided by the Shelf Management.
D channel cannot be established	
DEBUG mode enabled	Possible explanations: • System is running in DEBUG mode. • System DEBUG mode initiated. In this mode, additional prints are added and Startup and Recovery Conditions are different then Non Debug Mode. Change the DEBUG_MODE flag value to NO and reset the Collaboration Server.
DEBUG mode flags in use	The system is using the DEBUG CFG flags.
DMA not supported by IDE device	Possible explanations: • DMA (direct memory access) not supported by IDE device: Incompatible flash card / hard disk being used. • Flash card / hard drive are not properly connected to the board / one of the IDE channels is disconnected. • DMA was manually disabled for testing.
DNS configuration error	Check the DNS configuration.
DNS not configured in IP Network Service	Configure the DNS in the IP Network Services.
Encryption Server Error. Failed to generate the encryption key	FIPS 140 test failed while generating the new encryption key.
Error in external database certificate	

Table B-1   *Active Alarms (Continued)*

Alarm Code	Alarm Description
Error reading MCU time	Failed to read MCU time configuration file ([status]). Manually configure the MCU Time in the Collaboration Server Web Client or RMX Manager Manager application.
eUserMsgCode_Cs_EdgeServerDnsFailed	
eUserMsgCode_Cs_SipTLS_CertificateHasExpired	
eUserMsgCode_Cs_SipTLS_CertificateSubjNameIsNotValid_Or_DnsFailed	
eUserMsgCode_Cs_SipTLS_CertificateWillExpireInLessThanAWeek	
eUserMsgCode_Cs_SipTLS_FailedToLoadOrVerifyCertificateFiles	
eUserMsgCode_Cs_SipTLS_RegistrationHandshakeFailure	
eUserMsgCode_Cs_SipTLS_RegistrationServerNotResponding	
Event Mode Conferencing resources deficiency due to inappropriate license. Please install a new license	
External NTP servers failure	The MCU could not connect to any of the defined NTP server for synchronization due to the remote server error or network error or configuration error. Change the configuration of the NTP server.
Failed to access DNS server	Failed to access DNS server.
Failed to configure the Media card IP address	Possible reasons for the failure: • Failure type: [OK Or Not supported. • Does not exist Or IP failure. • Duplicate IP Or DHCP failure. • VLAN failure Or Invalid: [status_Number].
Failed to configure the Users list in Linux	The authentication process did not start. Use the Restore to factory Defaults to recover.
Failed to connect to application server	Possible reasons for the failure: • Failed to connect to application server: • Failed to establish connection to server, url = [url].
Failed to connect to recording device	The MCU could not connect to the defined recording device due to configuration error or network error.
Failed to connect to SIP registrar	Cannot establish connection with SIP registrar.

Table B-1   *Active Alarms (Continued)*

Alarm Code	Alarm Description
Failed to create Default Profile	Possible reasons for the failure: • Failed to validate the default Profile. • Failed to add the default Profile. Possible action: • Restore the Collaboration Server configuration from the Backup. • Use the Non-Comprehensive Restore To Factory Defaults operation.
Failed to initialize system base mode	
Failed to initialize the file system	Possible reasons for the failure: • Failed to initialize the file system. • Failed to initialize the file system and create the CDR index. Reset the MCU.
Failed to open Users list file	Restore the MCU configuration or re-define the user.
Failed to register with DNS server	Check the DNS configuration.
Failed to subscribe with the OCS, therefore the A/V Edge Server URI was not received	
Failure in initialization of SNMP agent.	
Fallback version is being used	Fallback version is being used. Restore current version. Version being used: [running version]; Current version: [current version].
Fan Problem Level Critical	
Fan Problem Level Major	
File error	Possible reasons for the file error: • XML file does not exist [file name]; Error no: [error number]. • Not authorized to open XML file [file name]; Error no: [error number]. • Unknown problem in opening XML file [file name]; Error no: [error number]. • Failed to parse XML file [file name].
File system scan failure	File system scan failure: Failed to scan [file system path]. Multiple occurrences may point to a hardware problem. System is functioning.
File system space shortage	File system space shortage: Out of file system space in [file system path]; Free space: [free space percentage]% ([free space] Blocks) - Minimum free space required: [minimum free space percentage]% ([minimum free space] Blocks).
FIPS 140 failure	
FIPS 140 test result not received	

Table B-1 *Active Alarms (Continued)*

Alarm Code	Alarm Description

Gatekeeper failure	Possible reasons for the Gatekeeper failure:
	• Failed to register to alternate Gatekeeper.
	• Gatekeeper discovery state.
	    - Check GK IP address (GUI, ping)
	• Gatekeeper DNS Host name not found.
	• Gatekeeper Registration Timeout.
	• Gatekeeper rejected GRQ due to invalid revision.
	• Gatekeeper rejected GRQ due to resource unavailability.
	• Gatekeeper rejected GRQ due to Terminal Exclusion.
	• Gatekeeper rejected GRQ due to unsupported feature.
	• Gatekeeper rejected GRQ. Reason 18.
	• Gatekeeper rejected RRQ due to Discovery Required.
	• Gatekeeper rejected RRQ due to duplicate alias.
	    - Check duplicate in aliases or in prefixes
	• Gatekeeper rejected RRQ due to Generic Data.
	• Gatekeeper rejected RRQ due to invalid alias.
	• Gatekeeper rejected RRQ due to invalid call signaling address.
	• Gatekeeper rejected RRQ due to invalid endpoint ID.
	• Gatekeeper rejected RRQ due to invalid RAS address.
	• Gatekeeper rejected RRQ due to invalid revision.
	• Gatekeeper rejected RRQ due to invalid state.
	• Gatekeeper rejected RRQ due to invalid terminal alias.
	• Gatekeeper rejected RRQ due to resource unavailability.
	• Gatekeeper rejected RRQ due to Security Denial.
	• Gatekeeper rejected RRQ due to terminal type.
	• Gatekeeper rejected RRQ due to unsupported Additive Registration.
	• Gatekeeper rejected RRQ due to unsupported feature.
	• Gatekeeper rejected RRQ due to unsupported QOS transport.
	• Gatekeeper rejected RRQ due to unsupported transport.
	• Gatekeeper rejected RRQ. Full registration required.
	• Gatekeeper rejected RRQ. Reason 18.
	• Gatekeeper Unregistration State.
	• Registration succeeded.
	Check the Gatekeeper configuration.

GUI System configuration file is invalid xml file	The XML format of the system configuration file that contains the user interface settings is invalid.
Hard disk error	Hard disk not responding.
Hot Backup: Master-Slave configuration conflict.	Possible reasons: • When both the MCUs are configured as Master or as Slave • The slave Collaboration Server is defined with the same IP as the Master.
Hot backup: Network issue	

Table B-1   *Active Alarms (Continued)*

Alarm Code	Alarm Description
Hot Backup: Paired MCU is unreachable.	
Initialization of ice stack failed	
Insufficient resources	The number of resources in the license is higher than the actual system resources. Check the media cards or insert a media card.
Insufficient UDP Ports	When defining fixed port, the number of defined UDP ports is lower than the required ports. Configure additional ports.
Internal System configuration during startup	System configuration during startup. Wait until Collaboration Server startup is completed.
Invalid System Configuration	
IP addresses of Signaling Host and Control Unit are the same	IP addresses of Signaling Host and Control Unit are identical. Assign different IP addresses to the Signaling Host and Control Unit.
IP Network Service added	
IP Network Service configuration modified	IP Network Service was modified. Reset the MCU.
IP Network Service deleted	IP Network Service was deleted. Reset the MCU.
IP Network Service not found	IP Service not found in the Network Services list. Configure the IP Network Service.
IPMC software upgrade in component	
IPS 140 test result not received	
LDAP TLS: Failed to connect to OSCP responder	
License not found	Possible causes: • The Central Signaling component could not find the IP Services after startup. • During Startup, the resources did not get the License required to utilize their Units. Possible action: • Configure IP service if not configure. • Reset the MCU. • Change the license
Management Network not configured	Configure the Management Network.
Missing Central Signaling configuration	Configure the central signaling.
Missing Central Signaling IP configuration	

Table B-1   *Active Alarms (Continued)*

Alarm Code	Alarm Description
MPL startup failure. Authentication not received.	Authentication was not received from Switch. Check the switch card.
MPL startup failure. Management Network configuration not received.	Management Network message was not received. Check the Switch card.
Network interface is not configured. New interface need to be chosen	
Network traffic capture is on	
New certificate for CS need Collaboration Server reset to take effect	
No default IVR Service in IVR Services list	No default IVR Service in IVR Services list. Ensure that one conference IVR Service and one EQ IVR Service are set as default.
No IP Network Services defined	IP Network Service parameters missing. Configure the IP Network Service.
No LAN connection	
No response from Central Signaling	No connection with central signaling.
No RTM-LAN or RTM-ISDN installed. One of these cards must be installed in the RealPresence Collaboration Server (RMX) 4000	
No usable unit for audio controller	No media card is installed, or the media card installed is not functioning. Install the appropriate media card.
OCS Registration failed	
Password expiration warning	
Please install a newer version	
Port configuration was modified	
Power off	
Power Problem Level Critical	
Power Problem Level Major	
Product activation failure	Assign a new activation key.
Product Type mismatch. System is restarting.	The user is alerted to a mismatch between the product type that is stored in MCU software and the product type received from another system component. In such a case the system is automatically restarted.
Received Notification failed	
Recording device has disconnected unexpectedly	

Table B-1   *Active Alarms (Continued)*

Alarm Code	Alarm Description
Requested changes to the certification repository were not completed. Repository must be updated to implement these changes.	
Resource process failed to request the Meeting Room list during startup.	Without the Meeting Rooms list, the system cannot allocate the appropriate dial numbers, Conference ID etc. and therefore cannot run conferences.
Restore Failed	Restoring the system configuration has failed as the system could not locate the configuration file in the selected path, or could not open the file.
Restore Succeeded	Restoring the system configuration has succeeded. Reset the MCU.
Restoring Factory Defaults. Default system settings will be restored once Reset is completed	Default system settings will be restored once Reset is completed.
Collaboration Server fails to connect to Active Directory server.	
Collaboration Server is uploading the version file. To cancel the upload and the upgrade, reset the Collaboration Server	
Collaboration Server user/password list will be reset	
Secured SIP communication failed	Error status (408) received from SIP proxy.
Security mode failed. Certificate has expired.	
Security mode failed. Certificate host name does not match the Collaboration Server host name.	
Security mode failed. Certificate is about to expire.	
Security mode failed. Certificate not yet valid.	
Security mode failed. Error in certificate file.	
Service Request failed	
SIP registrations limit reached	SIP registrations limit reached.
SIP TLS: Certificate has expired	The current TLS certificate files have expired and must be replaced with new files.
SIP TLS: Certificate is about to expire	The current TLS certificate files will expire shortly and will have to be replaced to ensure the communication with the OCS.
SIP TLS: Certificate subject name is not valid or DNS failed to resolve this name	This alarm is displayed if the name of the Collaboration Server in the certificate file is different from the FQDN name defined in the OCS.

Table B-1 *Active Alarms (Continued)*

Alarm Code	Alarm Description
SIP TLS: Failed to load or verify certificate files	This alarm indicates that the certificate files required for SIP TLS could not be loaded to the Collaboration Server. Possible causes are: • Incorrect certificate file name. Only files with the following names can be loaded to the system: rootCA.pem, pkey.pem, cert.pem and certPassword.txt • Wrong certificate file type. Only files of the following types can be loaded to the system: rootCA.pem, pkey.pem and cert.pem and certPassword.txt • The contents of the certificate file does not match the system parameters
SIP TLS: Registration handshake failure	This alarm indicates a mismatch between the security protocols of the OCS and the Collaboration Server, preventing the Registration of the Collaboration Server to the OCS.
SIP TLS: Registration server not responding	This alarm is displayed when the Collaboration Server does not receive a response from the OCS to the registration request in the expected time frame. Possible causes are: • The Collaboration Server FQDN name is not defined in the OCS pool, or is defined incorrectly. • The time frame for the expected response was too short and it will be updated with the next data refresh. The alarm may be cleared automatically the next time the data is refreshed. • The Collaboration Server FQDN name is not defined in the DNS server. Ping the DNS using the Collaboration Server FQDN name to ensure that the Collaboration Server is correctly registered to the DNS.
SIP TLS: Registration transport error	This alarm indicates that the communication with the SIP server cannot be established. Possible causes are: • Incorrect IP address of the SIP server • The SIP server listening port is other than the one defined in the system • The OCS services are stopped
Software upgrade in component	
SSH is enabled	
SWITCH not responding	Check the Switch card.
System Cards MPM Plus mode are not supported in Event mode	
System configuration changed. Please reset the MCU	
System Configuration modified	System configuration flags were modified. Reset the MCU.
System resources of Audio ports usage has exceeded Port Gauge threshold	
System resources of Video ports usage has exceeded Port Gauge threshold	

Table B-1   *Active Alarms (Continued)*

Alarm Code	Alarm Description
System resources usage has exceeded Port Gauge threshold	
Temperature Level - Critical	Possible explanations: • Temperature has reached a critical level.
Temperature Level - Major	Possible explanations: • Temperature has reached a problematic level and requires attention.
The Log file system is disabled because of high system CPU usage	
The MCCF channel is not connected	
The software contains patch(es)	The software contains patch(es).
Unable to connect to Exchange Server.	
User Name SUPPORT cannot be used in Enhanced Security Mode	
Version upgrade is in progress	
Voltage problem	Possible reasons for the problem: • Card voltage problem. • Voltage problem
Warning: Upgrade started and SAFE Upgrade protection is turned OFF	
Yellow Alarm	Problem sending/receiving data from/to network. Check the cables.

Appendix C

CDR Fields - Unformatted File

The CDR (Call Detail Records) utility is used to retrieve conference information to a file. The CDR utility can retrieve conference information to a file in both formatted and unformatted formats.

Unformatted CDR files contain multiple records. The first record in each file contains information about the conference in general, such as the conference name and start time. The remaining records each contain information about one event that occurred during the conference, such as a participant connecting to the conference, or a user extending the length of the conference. The first field in each record identifies the event type, and this is followed by values containing information about the event. The fields are separated by commas.

Formatted files contain basically the same information as unformatted files, but with the field values replaced by descriptions. Formatted files are divided into sections, each containing information about one conference event. The first line in each section is a title describing the type of event, and this is followed by multiple lines, each containing information about the event in the form of a descriptive field name and value.

> The field names and values in the formatted file will appear in the language being used for the *Collaboration Server Web Client* user interface at the time when the CDR information is retrieved. The value of the fields that support Unicode values, such as the info fields, will be stored in the CDR file in UTF8. The application that reads the CDR file must support Unicode.

The MCU sends the entire CDR file via API or HTTP, and the Collaboration Server or external application does the processing and sorting. The Collaboration Server ignores events that it does not recognize, that is, events written in a higher version that do not exist in the current version. Therefore, to enable compatibility between versions, instead of adding new fields to existing events, new fields are added as separate events, so as not to affect the events from older versions. This allows users with lower versions to retrieve CDR files that were created in higher versions.

> This appendix describes the fields and values in the unformatted CDR records.
> Although the formatted files contain basically the same information, in a few instances a single field in the unformatted file is converted to multiple lines in the formatted file, and in other cases, multiple fields in the unformatted file are combined into one line in the formatted file.
> In addition, to enable compatibility for applications that were written for the MGC family, the unformatted file contains fields that were supported by the MGC family, but are not supported by the Collaboration Server, whereas these fields are omitted from the formatted file.

The Conference Summary Record

The conference summary record (the first record in the unformatted CDR file) contains the following fields:

Table C-1   Conference Summary Record Fields

Field	Description
File Version	The version of the CDR utility that created the file.
Conference Routing Name	The Routing Name of the conference.
Internal Conference ID	The conference identification number as assigned by the system.
Reserved Start Time	The time the conference was scheduled to start in Greenwich Mean Time (GMT). The reservation time of a reservation that was started immediately or of an ongoing conference is the same as the *Actual Start Time*.
Reserved Duration	The amount of time the conference was scheduled to last.
Actual Start Time	The actual time the conference started in GMT.
Actual Duration	The actual conference duration.
Status	The conference status code as follows: **1** - The conference is an ongoing conference. **2** - The conference was terminated by a user. **3** - The conference ended at the scheduled end time. **4** - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. **5** - The conference never started. **6** - The conference could not start due to a problem. **8** - An unknown error occurred. **9** - The conference was terminated by a participant using DTMF codes. **Note:** If the conference was terminated by an MCU reset, this field will contain the value **1** (ongoing conference).
File Name	The name of the conference log file.
GMT Offset Sign	Indicates whether the *GMT Offset* is positive or negative. The possible values are: **0** - Offset is negative. GMT Offset will be subtracted from the GMT Time. **1** - Offset is positive. GMT Offset will be added to the GMT Time.

Table C-1   Conference Summary Record Fields (Continued)

Field	Description
GMT Offset	The time zone difference between Greenwich and the Collaboration Server's physical location in hours and minutes. Together with the *GMT Offset Sign* field the *GMT Offset* field is used to define the Collaboration Server local time. For example, if the *GMT Offset Sign* is 0 and *GMT Offset* is 3 hours then the time zone of the Collaboration Server's physical location is -3, which will be subtracted from the GMT time to determine the local time. However, if the *GMT Offset Sign* is 1 and *GMT Offset* is 4 hours then the time zone of the Collaboration Server's physical location is +4, which will be added to the GMT time to determine the local time.
File Retrieved	Indicates if the file has been retrieved and saved to a formatted file, as follows: **0** - No **1** - Yes

Event Records

The event records, that is, all records in the unformatted file except the first record, contain standard fields, such as the event type code and the time stamp, followed by fields that are event specific.

The event fields are separated by commas. Two consecutive commas with nothing between them (,,), or a comma followed immediately by a semi-colon (,;), indicates an empty field, as in the example below:

Standard Event Record Fields

All event records start with the following fields:
- The CDR event type code. For a list of event type codes and descriptions, refer to Table C-2, "*CDR Event Types,*" on page **C-4**.
- The event date.
- The event time.
- The structure length. This field is required for compatibility purposes, and always contains the value **0**.

Event Types

The table below contains a list of the events that can be logged in the CDR file, and indicates where to find details of the fields that are specific to that type of event.

> The event code identifies the event in the unformatted CDR file, and the event name identifies the event in the formatted CDR file.

Table C-2 *CDR Event Types*

Event Code	Event Name	Description
1	*CONFERENCE START*	The conference started. For more information about the fields, see Table C-3, "*Event Fields for Event 1 - CONFERENCE START,"* on page **C-10**. **Note:** There is one CONFERENCE START event per conference. It is always the first event in the file, after the conference summary record. It contains conference details, but not participant details.
2	*CONFERENCE END*	The conference ended. For more information about the fields, see Table C-8, "*Event Fields for Event 2 - CONFERENCE END,"* on page **C-15**. **Note:** There is one CONFERENCE END event per conference, and it is always the last event in the file.
7	*PARTICIPANT DISCONNECTED*	A participant disconnected from the conference. For more information about the fields, see Table C-11, "*Event Fields for Event 7 - PARTICIPANT DISCONNECTED,"* on page **C-15**.
10	*DEFINED PARTICIPANT*	Information about a defined participant, that is, a participant who was added to the conference before the conference started. For more information about the fields, see Table C-13, "*Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT,"* on page **C-16**. **Note:** There is one event for each participant defined before the conference started.
15	*H323 CALL SETUP*	Information about the IP address of the participant. For more information about the fields, see Table C-16, "*Event fields for Event 15 - H323 CALL SETUP,"* on page **C-19**.
17	*H323 PARTICIPANT CONNECTED*	An H.323 participant connected to the conference. For more information about the fields, see Table C-17, "*Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED,"* on page **C-20**.

Table C-2   *CDR Event Types (Continued)*

Event Code	Event Name	Description
18	*NEW UNDEFINED PARTICIPANT*	A new undefined participant joined the conference. For more information about the fields, see Table C-18, "*Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT,*" on page **C-22**.
20	*BILLING CODE*	A billing code was entered by a participant using DTMF codes. For more information about the fields, see Table C-20, "*Event Fields for Event 20 - BILLING CODE,*" on page **C-24**.
21	*SET PARTICIPANT DISPLAY NAME*	A user assigned a new name to a participant, or an end point sent its name. For more information about the fields, see Table C-21, "*Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME,*" on page **C-25**.
22	*DTMF CODE FAILURE*	An error occurred when a participant entered a DTMF code. For more information about the fields, see Table C-22, "*Event Fields for Event 22 - DTMF CODE FAILURE,*" on page **C-25**.
23	*SIP PARTICIPANT CONNECTED*	A SIP participant connected to the conference. For more information about the fields, see Table C-17, "*Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED,*" on page **C-20**.
26	*RECORDING LINK*	A recording event, such as recording started or recording resumed, occurred. For more information about the fields, see Table C-23, "*Event fields for Event 26 - RECORDING LINK,*" on page **C-25**.
28	*SIP PRIVATE EXTENSIONS*	Contains SIP Private Extensions information. For more information about the fields, see Table C-24, "*Event Fields for Event 28 - SIP PRIVATE EXTENSIONS,*" on page **C-26**.
30	*GATEKEEPER INFORMATION*	Contains the gatekeeper caller ID, which makes it possible to match the CDR in the gatekeeper and in the MCU. For more information about the fields, see Table C-25, "*Event Fields for Event 30 - GATEKEEPER INFORMATION,*" on page **C-26**.
31	*PARTICIPANT CONNECTION RATE*	Information about the line rate of the participant connection. This event is added to the CDR file each time the endpoint changes its connection bit rate. For more information about the fields, see Table C-26, "*Event fields for Event 31 - PARTICIPANT CONNECTION RATE,*" on page **C-26**.

Table C-2   *CDR Event Types (Continued)*

Event Code	Event Name	Description
33	*PARTY CHAIR UPDATE*	Participants connect to the conferences as standard participants and they are designated as chairpersons either by entering the chairperson password during the IVR session upon connection, or while participating in the conference using the appropriate DTM code. For more information about the fields, see see "*Event fields for Event 33 - PARTY CHAIR UPDATE*" on page **C-27**.
34	*PARTICIPANT MAXIMUM USAGE INFORMATION*	This event includes information of the maximum line rate, maximum resolution and maximum frame rate used by H.323 or SIP participant during the conference.
100	*USER TERMINATE CONFERENCE*	A user terminated the conference. For more information about the fields, see Table C-31, "*Event Fields for Event 100 - USER TERMINATE CONFERENCE,*" on page **C-28**.
101	*USER ADD PARTICIPANT*	A user added a participant to the conference during the conference. For more information about the fields, see Table C-13, "*Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT,*" on page **C-16**.
102	*USER DELETE PARTICIPANT*	A user deleted a participant from the conference. For more information about the fields, see Table C-32, "*Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT,*" on page **C-28**.
103	*USER DISCONNECT PARTICIPANT*	A user disconnected a participant. For more information about the fields, see Table C-32, "*Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT,*" on page **C-28**.
104	*USER RECONNECT PARTICIPANT*	A user reconnected a participant who was disconnected from the conference. For more information about the fields, see Table C-32, "*Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT,*" on page **C-28**.

Table C-2   *CDR Event Types (Continued)*

Event Code	Event Name	Description
105	*USER UPDATE PARTICIPANT*	A user updated the properties of a participant during the conference. For more information about the fields, see Table C-13, "*Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT,*" on page **C-16**.
106	*USER SET END TIME*	A user modified the conference end time. For more information about the fields, see Table C-33, "*Event Fields for Event 106 - USER SET END TIME,*" on page **C-29**.
107	*OPERATOR MOVE PARTY FROM CONFERENCE*	The participant moved from an Entry Queue to the destination conference or between conferences. For more information about the fields, see Table C-34, "*Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY,*" on page **C-29**.
108	*OPERATOR MOVE PARTY TO CONFERENCE*	The Collaboration Server User moved the participant from an ongoing conference to another conference. For more information, see Table C-35, "*Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE,*" on page **C-29**.
109	*OPERATOR ATTEND PARTY*	The Collaboration Server User moved the participant to the Operator conference. For more information, see Table C-34, "*Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY,*" on page **C-29**.
111	*OPERATOR BACK TO CONFERENCE PARTY*	The Collaboration Server User moved the participant back to his Home (source) conference. For more information, see Table C-36, "*Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY,*" on page **C-33**.
112	*OPERATOR ATTEND PARTY TO CONFERENCE*	The Collaboration Server User moved the participant from the Operator conference to another conference. For more information, see Table C-35, "*Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE,*" on page **C-29**.
1001	*NEW UNDEFINED PARTICIPANT CONTINUE 1*	Additional information about a NEW UNDEFINED PARTICIPANT event. For more information about the fields, see Table C-19, "*Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1,*" on page **C-24**.

Table C-2 *CDR Event Types (Continued)*

Event Code	Event Name	Description
2001	*CONFERENCE START CONTINUE 1*	Additional information about a CONFERENCE START event. For more information about the fields, see Table C-4, "*Event Fields for Event 2001 - CONFERENCE START CONTINUE 1,*" on page **C-11**.
2007	*PARTICIPANT DISCONNECTED CONTINUE 1*	Additional information about a PARTICIPANT DISCONNECTED event. For more information about the fields, see Table C-12, "*Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1,*" on page **C-15**.
2010	*DEFINED PARTICIPANT CONTINUE 1*	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Table C-14, "*Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1,*" on page **C-18**.
2011	*RESERVED PARTICIPANT CONTINUE PV6 ADDRESS*	Additional information about a DEFINED PARTICIPANT event that includes the IPv6 addressing of the defined participant. For more details, see "*Event Fields for Events 2011, 2012, and 2016*" on page **C-33**.
2012	*RESERVED PARTICIPANT CONTINUE 2*	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Table C-15, "*Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2,*" on page **C-19**.
2101	*USER ADD PARTICIPANT CONTINUE 1*	Additional information about a USER ADD PARTICIPANT event. For more information about the fields, see Table C-14, "*Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1,*" on page **C-18**.
2102	*USER ADD PARTICIPANT CONTINUE 2*	Additional information about a USER ADD PARTICIPANT event. For more information about the fields, see Table C-15, "*Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2,*" on page **C-19**.
2105	*USER UPDATE PARTICIPANT CONTINUE 1*	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Table C-14, "*Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1,*" on page **C-18**.

Table C-2 *CDR Event Types (Continued)*

Event Code	Event Name	Description
2106	*USER UPDATE PARTICIPANT CONTINUE 2*	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Table C-15, "*Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2,*" on page **C-19**.
3010	*PARTICIPANT INFORMATION*	The contents of the participant information fields. For more information about the fields, see Table C-38, "*Event Fields for Event 3010 - PARTICIPANT INFORMATION,*" on page **C-33**.
5001	*CONFERENCE START CONTINUE 4*	Additional information about a CONFERENCE START event. For more information about the fields, see Table C-5, "*Event Fields for Event 5001 - CONFERENCE START CONTINUE 4,*" on page **C-13**. **Note:** An additional CONFERENCE START CONTINUE 4 event will be written to the CDR each time the value of one of the following conference fields is modified: • Conference Password • Chairperson Password • Info1, Info2 or Info3 • Billing Info These additional events will only contain the value of the modified field.
6001	*CONFERENCE START CONTINUE 5*	Additional information about a CONFERENCE START event. For more information about the fields, see Table C-6, "*Event Fields for Event 6001 - CONFERENCE START CONTINUE 5,*" on page **C-14**.
11001	*CONFERENCE START CONTINUE 10*	Additional information about a CONFERENCE START event. This event contains the Display Name. For more information about the fields, see Table C-7, "*Event Fields for Event 11001 - CONFERENCE START CONTINUE 10,*" on page **C-14**.

This list only includes events that are supported by the Collaboration Server. For a list of MGC Manager events that are not supported by the Collaboration Server, see "*MGC Manager Events that are not Supported by the Collaboration Server*" on page **C-36**.

Event Specific Fields

The following tables describe the fields which are specific to each type of event.

> Some fields that were supported by the MGC Manager, are not supported by the Collaboration Server. In addition, for some fields the Collaboration Server has a fixed value, whereas the MGC Manager supported multiple values. For more information about the MGC Manager fields and values, see the *MGC Manager User's Guide Volume II*, *Appendix A*.

Table C-3   *Event Fields for Event 1 - CONFERENCE START*

Field	Description
Dial-Out Manually	Indicates whether the conference was a dial-out manually conference or not. Currently the only value is: **0** - The conference was *not* a dial-out manually conference, that is, the MCU initiates the communication with dial-out participants, and the user does not need to connect them manually.
Auto Terminate	Indicates whether the conference was set to end automatically if no participant joins the conference for a predefined time period after the conference starts, or if all participants disconnect from the conference and the conference is empty for a predefined time period. Possible values are: **0** - The conference was *not* set to end automatically. **1** - The conference was set to end automatically.
Line Rate	The conference line rate, as follows: **0** - 64 kbps **6** - 384 kbps **12** - 1920 kbps **13** - 128 kbps **15** - 256 kbps **23** - 512 kbps **24** - 768 kbps **26** - 1152 kbps **29** - 1472 kbps **32** - 96 kbps
Line Rate (cont.)	**33** - 1024 kbps **34** - 4096 kbps
Restrict Mode	Not supported. Always contains the value **0**.
Audio Algorithm	The audio algorithm. Currently the only value is: **255** - Auto
Video Session	The video session type. Currently the only value is: **3** - Continuous Presence
Video Format	The video format. Currently the only value is: **255** - Auto

Table C-3   *Event Fields for Event 1 - CONFERENCE START (Continued)*

Field	Description
CIF Frame Rate	The CIF frame rate. Currently the only value is: **255** -Auto
QCIF Frame Rate	The QCIF frame rate: Currently the only value is: **255** - Auto
LSD Rate	Not supported. Always contains the value **0**.
HSD Rate	Not supported. Always contains the value **0**.
T120 Rate	Not supported. Always contains the value **0**.

Table C-4   *Event Fields for Event 2001 - CONFERENCE START CONTINUE 1*

Field	Description
Audio Tones	Not supported. Always contains the value **0**.
Alert Tone	Not supported. Always contains the value **0**.
Talk Hold Time	The minimum time that a speaker has to speak to become the video source. The value is in units of 0.01 seconds. Currently the only value is **150**, which indicates a talk hold time of 1.5 seconds.
Audio Mix Depth	The maximum number of participants whose audio can be mixed. Currently the only value is **5**.
Operator Conference	Not supported. Always contains the value **0**.
Video Protocol	The video protocol. Currently the only value is: **255** - Auto
Meet Me Per Conference	Indicates the Meet Me Per Conference setting. Currently the only value is: **1** - The Meet Me Per Conference option is enabled, and dial-in participants can join the conference by dialing the dial-in number.
Number of Network Services	Not supported. Always contains the value **0**.

Table C-4 *Event Fields for Event 2001 - CONFERENCE START CONTINUE 1 (Continued)*

Field	Description
Chairperson Password	The chairperson password for the conference. An empty field "" means that no chairperson password was assigned to the conference.
Chair Mode	Not supported. Always contains the value **0**.
Cascade Mode	The cascading mode. Currently the only value is: **0** - None
Master Name	Not supported. This field remains empty.
Minimum Number of Participants	The number of participants for which the system reserved resources. Additional participants may join the conference without prior reservation until all the resources are utilized. Currently the only value is **0**.
Allow Undefined Participants	Indicates whether or not undefined dial-in participants can connect to the conference. Currently the only value is: **1** - Undefined participants can connect to the conference
Time Before First Participant Joins	**Note:** This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse from the time the conference starts, without any participant connecting to the conference, before the conference is automatically terminated by the MCU.
Time After Last Participant Quits	**Note:** This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse after the last participant has disconnected from the conference, before the conference is automatically terminated by the MCU.
Conference Lock Flag	Not supported. Always contains the value **0**.
Maximum Number of Participants	The maximum number of participants that can connect to the conference at one time. The value **65535** (auto) indicates that as many participants as the MCU's resources allow can connect to the conference, up to the maximum possible for the type of conference.
Audio Board ID	Not supported. Always contains the value **65535**.
Audio Unit ID	Not supported. Always contains the value **65535**.
Video Board ID	Not supported. Always contains the value **65535**.

Table C-4   *Event Fields for Event 2001 - CONFERENCE START CONTINUE 1 (Continued)*

Field	Description
Video Unit ID	Not supported. Always contains the value **65535**.
Data Board ID	Not supported. Always contains the value **65535**.
Data Unit ID	Not supported. Always contains the value **65535**.
Message Service Type	The Message Service type. Currently the only value is: **3** - IVR
Conference IVR Service	The name of the IVR Service assigned to the conference. **Note:** If the name of the IVR Service contains more than 20 characters, it will be truncated to 20 characters.
Lecture Mode Type	Indicates the type of Lecture Mode, as follows: **0** - None **1** - Lecture Mode **3** - Presentation Mode
Lecturer	**Note:** This field is only relevant if the Lecture Mode Type is Lecture Mode. The name of the participant selected as the conference lecturer.
Time Interval	**Note:** This field is only relevant if Lecturer View Switching is enabled. The number of seconds a participant is to be displayed in the lecturer window before switching to the next participant. Currently the only value is **15**.
Lecturer View Switching	**Note:** This field is only relevant when Lecture Mode is enabled. Indicates the lecturer view switching setting, as follows: **0** - Automatic switching between participants is disabled. **1** - Automatic switching between participants is enabled.
Audio Activated	Not supported. Always contains the value **0**.
Lecturer ID	Not supported. Always contains the value **4294967295**.

Table C-5   *Event Fields for Event 5001 - CONFERENCE START CONTINUE 4*

Field	Description
Note: When this event occurs as the result of a change to the value of one of the event fields, the event will only contain the value of the modified field. All other fields will be empty.	
Conference ID	The conference ID.

Table C-5 *Event Fields for Event 5001 - CONFERENCE START CONTINUE 4 (Continued)*

Field	Description
Conference Password	The conference password. An empty field "" means that no conference password was assigned to the conference.
Chairperson Password	The chairperson password. An empty field "" means that no chairperson password was assigned to the conference.
Info1 *Info2* *Info3*	The contents of the conference information fields. These fields enable users to enter general information for the conference, such as the company name, and the contact person's name and telephone number. The maximum length of each field is 80 characters.
Billing Info	The billing code.

Table C-6 *Event Fields for Event 6001 - CONFERENCE START CONTINUE 5*

Field	Description
Encryption	Indicates the conference encryption setting, as follows: **0** - The conference is *not* encrypted. **1** - The conference is encrypted.

Table C-7 *Event Fields for Event 11001 - CONFERENCE START CONTINUE 10*

Field	Description
Display Name	The Display Name of the conference.

Table C-8 *Event Fields for Event 2 - CONFERENCE END*

Field	Description
Conference End Cause	Indicates the reason for the termination of the conference, as follows: **1** - The conference is an ongoing conference or the conference was terminated by an MCU reset. **2** - The conference was terminated by a user. **3** - The conference ended at the scheduled end time. **4** - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. **5** - The conference never started. **6** - The conference could not start due to a problem. **8** - An unknown error occurred. **9** - The conference was terminated by a participant using DTMF codes.

Table C-11 *Event Fields for Event 7 - PARTICIPANT DISCONNECTED*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Call Disconnection Cause	The disconnection cause. For more information about possible values, see Table C-39, "*Disconnection Cause Values,*" on page **C-33**.
Q931 Disconnect Cause	If the disconnection cause is "No Network Connection" or "Participant Hang Up", then this field indicates the Q931 disconnect cause.

Table C-12 *Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1*

Field	Description
Rx Synchronization Loss	The number of times that the general synchronization of the MCU was lost.
Tx Synchronization Loss	The number of times that the general synchronization of the participant was lost.
Rx Video Synchronization Loss	The number of times that the synchronization of the MCU video unit was lost.
Tx Video Synchronization Loss	The number of times that the synchronization of the participant video was lost.
Mux Board ID	Not supported. Always contains the value **0**.

Table C-12 *Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1*

Field	Description
Mux Unit ID	Not supported. Always contains the value **0**.
Audio Codec Board ID	Not supported. Always contains the value **0**.
Audio Codec Unit ID	Not supported. Always contains the value **0**.
Audio Bridge Board ID	Not supported. Always contains the value **0**.
Audio Bridge Unit ID	Not supported. Always contains the value **0**.
Video Board ID	Not supported. Always contains the value **0**.
Video Unit ID	Not supported. Always contains the value **0**.
T.120 Board ID	Not supported. Always contains the value **0**.
T.120 Unit ID	Not supported. Always contains the value **0**.
T.120 MCS Board ID	Not supported. Always contains the value **0**.
T.120 MCS Unit ID	Not supported. Always contains the value **0**.
H.323 Board ID	Not supported. Always contains the value **0**.
H323 Unit ID	Not supported. Always contains the value **0**.

Table C-13 *Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT*

Field	Description
User Name	The login name of the user who added the participant to the conference, or updated the participant properties.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Dialing Direction	The dialing direction, as follows: **0** - Dial-out **5** - Dial-in

Table C-13 *Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT (Continued)*

Field	Description
Bonding Mode	Not supported. Always contains the value **0**.
Number Of Channels	
Net Channel Width	Not supported. Always contains the value **0**.
Network Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Not supported. Always contains the value **0**.
Audio Only	Indicates the participant's Audio Only setting, as follows: **0** - The participant is *not* an Audio Only participant **1** - The participant is an Audio Only participant **255** - Unknown
Default Number Type	**Note:** This field is only relevant to ISDN/PSTN participants. The type of telephone number, as follows: **0** - Unknown **1** - International **2** - National **3** - Network specific **4** - Subscriber **6** - Abbreviated **255** - Taken from Network Service, default **Note:** For dial-in participants, the only possible value is: **255** - Taken from Network Service
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	
Number of MCU Phone Numbers	
Party and MCU Phone Numbers	

Table C-13 *Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT (Continued)*

Field	Description
Identification Method	**Note:** This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: **1** - Called IP address or alias **2** - Calling IP address or alias
Meet Me Method	**Note:** This field is only relevant to dial-in participants. The meet-me per method. Currently the only value is: **3** - Meet-me per participant

Table C-14 *Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1*

Field	Description
Network Type	The type of network between the participant and the MCU, as follows: **2** - H.323 **5** - SIP
H.243 Password	Not supported. This field remains empty.
Chair	Not supported. Always contains the value **0**.
Video Protocol	The video protocol used by the participant, as follows: **1** - H.261 **2** - H.263 **4** - H.264 **255** - Auto
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between **1** (lowest) and **10** (loudest). Each unit movement increases or decreases the volume by **3 dB**.
Undefined Participant	Indicates whether are not the participant is an undefined participant, as follows: **0** - The participant is *not* an undefined participant. **2** - The participant is an undefined participant.
Node Type	The node type, as follows: **0** - MCU **1** - Terminal
Bonding Phone Number	
Video Bit Rate	The video bit rate in units of kilobits per second. A value of **4294967295** denotes auto, and in this case, the rate is computed by the MCU.

Table C-14 *Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1,*
USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1

Field	Description
IP Address	The IP address of the participant. An address of **4294967295** indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Signaling Port	The signaling port used for participant connection.
H.323 Participant Alias Type/SIP Participant Address Type	For H.323 participants, the alias type, as follows: **7** - E164 **8** - H.323 ID **13** - Email ID **14** - Participant number For SIP participants, the address type, as follows: **1** - SIP URI **2** - Tel URL
H.323 Participant Alias Name/SIP Participant Address	For H.323 participants: The participant alias. The alias may contain up to 512 characters. For SIP participants: The participant address. The address may contain up to 80 characters.

Table C-15 *Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER*
ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT
CONTINUE 2

Field	Description
Encryption	Indicates the participant's encryption setting as follows: **0** - The participant is *not* encrypted. **1** - The participant is encrypted. **2** - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-16 *Event fields for Event 15 - H323 CALL SETUP*

Field	Description
Participant Name	The name of the participant.

Table C-16 *Event fields for Event 15 - H323 CALL SETUP (Continued)*

Field	Description
Participant ID	The identification number assigned to the participant by the MCU.
Connect Initiator	Indicates who initiated the connection, as follows: **0** - MCU **1** - Remote participant **Any other number** - Unknown
Min Rate	The minimum line rate used by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Max Rate	The maximum line rate achieved by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Source Party Address	The IP address of the calling participant. A string of up to 255 characters.
Destination Party Address	The IP address of the called participant. A string of up to 255 characters.
Endpoint Type	The endpoint type, as follows: **0** - Terminal **1** - Gateway **2** - MCU **3** - Gatekeeper **4** - Undefined

Table C-17 *Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED*

Field	Description
Participant Name	The name of the participant. An empty field "" denotes an unidentified participant or a participant whose name is unspecified.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-17 *Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED (Continued)*

Field	Description
Participant Status	The participant status, as follows: **0** - Idle **1** - Connected **2** - Disconnected **3** - Waiting for dial-in **4** – Connecting **5** - Disconnecting **6** - Partially connected. Party has completed H.221 capability exchange **7** - Deleted by a user **8** - Secondary. The participant could not connect the video channels and is connected via audio only **10** - Connected with problem **11** - Redialing
Capabilities	Not supported. Always contains the value **0**.
Remote Communication Mode	Not supported. Always contains the value **0**.
Secondary Cause	**Note:** This field is only relevant if the Participant Status is Secondary. The cause for the secondary connection (not being able to connect the video channels), as follows: 0 - Default **11** - The incoming video parameters are not compatible with the conference video parameters **13** - The conference video settings are not compatible with the endpoint capabilities **14** - The new conference settings are not compatible with the endpoint capabilities **15** - Video stream violation due to incompatible annexes or other discrepancy **16** - Inadequate video resources **17** - When moved to a Transcoding or Video Switching conference, the participant's video capabilities are not supported by the video cards **18** - Video connection could not be established **24** - The endpoint closed its video channels **25** - The participant video settings are not compatible with the conference protocol **26** - The endpoint could not re-open the video channel after the conference video mode was changed **27** - The gatekeeper approved a lower bandwidth than requested **28** - Video connection for the SIP participant is temporarily unavailable **255** - Other

Table C-18 Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Dialing Direction	The dialing direction, as follows **0** - Dial-out **5** - Dial-in
Bonding Mode	Not supported. Always contains the value **0**.
Number of Channels	
Net Channel Width	Not supported. Always contains the value **0**.
Network Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Not supported. Always contains the value **0**.
Audio Only	Indicates the participant's Audio Only setting, as follows: **0** - The participant is *not* an Audio Only participant **1** - The participant is an Audio Only participant **255** - Unknown
Default Number Type	
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	
Number of MCU Phone Numbers	
Party and MCU Phone Numbers	
Identification Method	**Note:** This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: **1** - Called IP address or alias **2** - Calling IP address or alias
Meet Me Method	**Note:** This field is only relevant to dial-in participants. The meet-me per method, as follows: **3** - Meet-me per participant

Table C-18 *Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT (Continued)*

Field	Description
Network Type	The type of network between the participant and the MCU, as follows: **2** - H.323 **5** - SIP
H.243 Password	Not supported. This field remains empty.
Chair	Not supported. Always contains the value **0**.
Video Protocol	The video protocol, as follows: **1** - H.261 **2** - H.263 **4** - H.264 **255** - Auto
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between **1** (lowest) and **10** (loudest). Each unit movement increases or decreases the volume by **3 dB**.
Undefined Participant	Indicates whether are not the participant is an undefined participant, as follows: **0** - The participant is *not* an undefined participant. **2** - The participant is an undefined participant.
Node Type	The node type, as follows: **0** - MCU **1** - Terminal
Bonding Phone Number	**Note:** This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls. Bonding is a communication protocol that aggregates from two up to thirty 64 Kbps B channels together, to look like one large bandwidth channel.
Video Bit Rate	The video bit rate in units of kilobits per second. A value of **4294967295** denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of **4294967295** indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection. A value of **65535** is ignored by MCU.

Table C-18 *Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT (Continued)*

Field	Description
H.323 Participant Alias Type/SIP Participant Address Type	For H.323 participants, the alias type, as follows: **7** - E164 **8** - H.323 ID **13** - Email ID **14** - Participant number For SIP participants, the address type, as follows: **1** - SIP URI **2** - Tel URL

H.323 Participant Alias Name/SIP Participant Address	For H.323 participants:
	  The participant alias.
	  The alias may contain up to 512 characters.
	
	For SIP participants:
	  The participant address.
	  The address may contain up to 80 characters.

Table C-19 *Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1*

Field	Description
Encryption	Indicates the participant's encryption setting as follows: **0** - The participant is *not* encrypted. **1** - The participant is encrypted. **2** - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-20 *Event Fields for Event 20 - BILLING CODE*

Field	Description
Participant Name	The name of the participant who added the billing code.
Participant ID	The identification number, as assigned by the MCU, of the participant who added the billing code.
Billing Info	The numeric billing code that was added (32 characters).

Table C-21 *Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME*

Field	Description
Participant Name	The original name of the participant, for example, the name automatically assigned to an undefined participant, such as, "<conference name>_(000)".
Participant ID	The identification number assigned to the participant by the MCU.
Display Name	The new name assigned to the participant by the user, or the name sent by the end point.

Table C-22 *Event Fields for Event 22 - DTMF CODE FAILURE*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Incorrect Data	The incorrect DTMF code entered by the participant, or an empty field "" if the participant did not press any key.
Correct Data	The correct DTMF code, if known.
Failure Type	The type of DTMF failure, as follows: **2** - The participant did not enter the correct conference password. **6** - The participant did not enter the correct chairperson password. **12** - The participant did not enter the correct Conference ID.

Table C-23 *Event fields for Event 26 - RECORDING LINK*

Field	Description
Participant Name	The name of the Recording Link participant.
Participant ID	The identification number assigned to the Recording Link participant by the MCU.
Recording Operation	The type of recording operation, as follows: **0** - Start recording **1** - Stop recording **2** - Pause recording **3** - Resume recording **4** - Recording ended **5** - Recording failed
Initiator	Not supported.

Table C-23 Event fields for Event 26 - RECORDING LINK (Continued)

Field	Description
Recording Link Name	The name of the Recording Link.
Recording Link ID	The Recording Link ID.
Start Recording Policy	The start recording policy, as follows: **1** - Start recording automatically as soon as the first participant connects to the conference. **2** - Start recording when requested by the conference chairperson via DTMF codes or from the *Collaboration Server Web Client*, or when the operator starts recording from the *Collaboration Server Web Client*.

Table C-24 Event Fields for Event 28 - SIP PRIVATE EXTENSIONS

Field	Description
Participant Name	The name of the participant.
Participant ID	The participant's identification number as assigned by the system.
Called Participant ID	The called participant ID.
Asserted Identity	The identity of the user sending a SIP message as it was verified by authentication.
Charging Vector	A collection of charging information.
Preferred Identity	The identity the user sending the SIP message wishes to be used for the P-Asserted-Header field that the trusted element will insert.

Table C-25 Event Fields for Event 30 - GATEKEEPER INFORMATION

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Gatekeeper Caller ID	The caller ID in the gatekeeper records. This value makes it possible to match the CDR in the gatekeeper and in the MCU.

Table C-26 Event fields for Event 31 - PARTICIPANT CONNECTION RATE

Field	Description
Participant Name	The participant name.

Table C-26 *Event fields for Event 31 - PARTICIPANT CONNECTION RATE (Continued)*

Field	Description
Participant ID	The identification number assigned to the participant by the MCU.
Participant Current Rate	The participant line rate in Kbps.

Table C-28 *Event fields for Event 33 - PARTY CHAIR UPDATE*

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Chairperson	Possible values: • True - participant is a chairperson • False - Participant is not a chairperson participant (is a standard participant)

Table C-29 *Event fields for Event 34 - PARTICIPANT MAXIMUM USAGE INFORMATION*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Maximum Bit Rate	The maximum bit rate used by the participant during the call.
Maximum Resolution	The maximum resolution used by the participant during the call. **Note:** The reported resolutions are: CIF, SD, HD720, and HD1080. Other resolutions are roundED up to the nearest resolution. For example, 2SIF is reported as SD resolution.
Maximum Frame Rate	The maximum frame rate used by the participant during the call.
Participant Address	For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

Table C-30 *Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED*

Field	Description
Participant Name	The name of the participant. An empty field "" denotes an unidentified participant or a participant whose name is unspecified

Table C-30 *Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED (Continued)*

Field	Description
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: 0 - Idle 1 - Connected 2 - Disconnected 3 - Waiting for dial-in 4 - Connecting 5 - Disconnecting 6 - Partially connected. Party has completed H.221 capability exchange 7 - Deleted by a user 8 - Secondary. The participant could not connect the video channels and is connected via audio only 10 - Connected with problem 11 - Redialing
Receive line rate	Negotiated reception line rate
Transmit line rate	Negotiated transmission line rate
Uplink Video Capabilities	a.Number of uplink streams b.Video stream (multiple streams) i.Resolution width ii.resolution height iii.max frame rate iv.max line rate
Audio Codec	SAC, Other
Secondary Cause	

Table C-31 *Event Fields for Event 100 - USER TERMINATE CONFERENCE*

Field	Description
Terminated By	The login name of the user who terminated the conference.

Table C-32 *Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT*

Field	Description
User Name	The login name of the user who reconnected the participant to the conference, or disconnected or deleted the participant from the conference.
Participant Name	The name of the participant reconnected to the conference, or disconnected or deleted from the conference.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-33 *Event Fields for Event 106 - USER SET END TIME*

Field	Description
New End Time	The new conference end time set by the user, in GMT time.
User Name	The login name of the user who changed the conference end time.

Table C-34 *Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY*

Field	Description
Operator Name	The login name of the user who moved the participant.
Party Name	The name of the participant who was moved.
Party ID	The identification number of the participant who was moved, as assigned by the MCU.
Destination Conf Name	The name of the conference to which the participant was moved.
Destination Conf ID	The identification number of the conference to which the participant was moved.

Table C-35 *Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE*

Field	Description
Operator Name	The login name of the operator who moved the participant to the conference.
Source Conf Name	The name of the source conference.
Source Conf ID	The identification number of the source conference, as assigned by the MCU.
Party Name	The name of the participant who was moved.
Party ID	The identification number assigned to the participant by the MCU.
Connection Type	The connection type, as follows: **0** - Dial-out **5** - Dial-in
Bonding Mode	
Number Of Channels	**Note:** This field is only relevant to ISDN/PSTN participants. The number of channels, as follows: **255** - Auto Otherwise, in range of **1** - **30**

*Table C-35 Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,
OPERATOR ATTEND PARTY TO CONFERENCE (Continued)*

Field	Description
Net Channel Width	The bandwidth of each channel. This value is always **0**, which represents a bandwidth of **1B**, which is the only bandwidth that is currently supported.
Net Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Indicates whether or not the line is restricted, as follows: **27** - Restricted line **28** - Non restricted line **255** - Unknown or not relevant
Voice Mode	Indicates whether or not the participant is an Audio Only participant, as follows: **0** - The participant is *not* an Audio Only participant **1** - The participant is an Audio Only participant **255** - Unknown
Number Type	**Note:** This field is only relevant to dial-out, ISDN/PSTN participants. The type of telephone number, as follows: **0** - Unknown **1** - International **2** - National **3** - Network specific **4** - Subscriber **6** - Abbreviated **255** - Taken from Network Service, default
Net SubService Name	**Note:** This field is only relevant to dial-out, ISDN/PSTN participants. The network sub-service name. An empty field "" means that MCU selects the default sub-service.
Number of Party Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of participant phone numbers. In a dial-in connection, the participant phone number is the CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, participant phone numbers are the phone numbers dialed by the MCU for each participant channel.
Number of MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of MCU phone numbers. In a dial-in connection, the MCU phone number is the number dialed by the participant to connect to the MCU. In a dial-out connection, the MCU phone number is the MCU (CLI) number as seen by the participant.

*Table C-35 Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,
OPERATOR ATTEND PARTY TO CONFERENCE (Continued)*

Field	Description
Party and MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The participant phone numbers are listed first, followed by the MCU phone numbers.
Ident. Method	**Note:** This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: **0** - Password **1** - Called phone number, or IP address, or alias **2** - Calling phone number, or IP address, or alias
Meet Method	**Note:** This field is only relevant to dial-in participants. The meet-me per method, as follows: **1** - Meet-me per MCU-Conference **3** - Meet-me per participant **4** - Meet-me per channel
Net Interface Type	The type of network interface between the participant and the MCU, as follows: **0** - ISDN **2** - H.323 **5** - SIP
H243 Password	The H.243 password, or an empty field "" if there is no password.
Chair	Not supported. Always contains the value **0**.
Video Protocol	The video protocol, as follows: **1** - H.261 **2** - H.263 **3** - H.264* **4** - H.264 **255** - Auto
Audio Volume	The broadcasting volume assigned to the participant. The value is between **1** (lowest) and **10** (loudest).
Undefined Type	The participant type, as follows: **0** - Defined participant. (The value in the formatted text file is "default".) **2** - Undefined participant. (The value in the formatted text file is "Unreserved participant ".)
Node Type	The node type, as follows: **0** - MCU **1** - Terminal
Bonding Phone Number	**Note:** This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls.

Table C-35 *Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE,*
OPERATOR ATTEND PARTY TO CONFERENCE (Continued)

Field	Description
Video Rate	**Note:** This field is only relevant to IP participants. The video rate in units of kilobits per second. A value of **4294967295** denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of **4294967295** indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Call Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection. A value of **65535** is ignored by MCU.
H.323 Party Alias Type/SIP Party Address Type	**Note:** This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: **7** - E164 **8** - H.323 ID **11** - URL ID alias type **12** - Transport ID **13** - Email ID **14** - Participant number For SIP participants, the address type, as follows: **1** - SIP URI **2** - Tel URL
H.323 Party Alias/ SIP Party Address	**Note:** This field is only relevant to IP participants. For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

Table C-36 *Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY*

Field	Description
Operator Name	The login name of the operator moving the participant back to the conference.
Party Name	The name of the participant being moved.
Party ID	The identification number, as assigned by the MCU, of the participant being moved.

Table C-37 *Event Fields for Events 2011, 2012, and 2016*

Field	Description
IP V6	IPv6 address of the participant's endpoint.

Table C-38 *Event Fields for Event 3010 - PARTICIPANT INFORMATION*

Field	Description
Info1 *Info2* *Info3* *Info4*	The participant information fields. These fields enable users to enter general information about the participant, such as the participant's e-mail address. The maximum length of each field is 80 characters.
VIP	Not supported. Always contains the value **0**.

Disconnection Cause Values

For an explanation of the disconnection causes, see *Appendix A:* "*Disconnection Causes"* on page **A-1**.

Table C-39 *Disconnection Cause Values*

Value	Call Disconnection Cause
0	Unknown
1	Participant hung up
2	Disconnected by User
5	Resources deficiency
6	Password failure
20	H323 call close. No port left for audio

Table C-39 *Disconnection Cause Values (Continued)*

Value	Call Disconnection Cause
21	H323 call close. No port left for video
22	H323 call close. No port left for FECC
23	H323 call close. No control port left
25	H323 call close. No port left for video content
51	A common key exchange algorithm could not be established between the MCU and the remote device
53	Remote device did not open the encryption signaling channel
59	The remote devices' selected encryption algorithm does not match the local selected encryption algorithm
141	Called party not registered
145	Caller not registered
152	H323 call close. ARQ timeout
153	H323 call close. DRQ timeout
154	H323 call close. Alt Gatekeeper failure
191	H323 call close. Remote busy
192	H323 call close. Normal
193	H323 call close. Remote reject
194	H323 call close. Remote unreachable
195	H323 call close. Unknown reason
198	H323 call close. Small bandwidth
199	H323 call close. Gatekeeper failure
200	H323 call close. Gatekeeper reject ARQ
201	H323 call close. No port left
202	H323 call close. Gatekeeper DRQ
203	H323 call close. No destination IP value
204	H323 call close. Remote has not sent capability
205	H323 call close. Audio channels not open
207	H323 call close. Bad remote cap
208	H323 call close. Capabilities not accepted by remote
209	H323 failure
210	H323 call close. Remote stop responding

Table C-39 *Disconnection Cause Values (Continued)*

Value	Call Disconnection Cause
213	H323 call close. Master slave problem
251	SIP timer popped out
252	SIP card rejected channels
253	SIP capabilities don't match
254	SIP remote closed call
255	SIP remote cancelled call
256	SIP bad status
257	SIP remote stopped responding
258	SIP remote unreachable
259	SIP transport error
260	SIP bad name
261	SIP trans error TCP invite
300	SIP redirection 300
301	SIP moved permanently
302	SIP moved temporarily
305	SIP redirection 305
380	SIP redirection 380
400	SIP client error 400
401	SIP unauthorized
402	SIP client error 402
403	SIP forbidden
404	SIP not found
405	SIP client error 405
406	SIP client error 406
407	SIP client error 407
408	SIP request timeout
409	SIP client error 409
410	SIP gone
411	SIP client error 411
413	SIP client error 413
414	SIP client error 414

Table C-39 Disconnection Cause Values (Continued)

Value	Call Disconnection Cause
415	SIP unsupported media type
420	SIP client error 420
480	SIP temporarily not available
481	SIP client error 481
482	SIP client error 482
483	SIP client error 483
484	SIP client error 484
485	SIP client error 485
486	SIP busy here
487	SIP request terminated
488	SIP client error 488
500	SIP server error 500
501	SIP server error 501
502	SIP server error 502
503	SIP server error 503
504	SIP server error 504
505	SIP server error 505
600	SIP busy everywhere
603	SIP global failure 603
604	SIP global failure 604
606	SIP global failure 606

MGC Manager Events that are not Supported by the Collaboration Server

The following MGC Manager events are not supported by the Collaboration Server:

For details of these events see the M*GC Manager User's Guide Volume II*, *Appendix A*.

- Event 8 - REMOTE COM MODE
- Event 11 - ATM CHANNEL CONNECTED
- Event 12 - ATM CHANNEL DISCONNECTED

- Event 13 - MPI CHANNEL CONNECTED
- Event 14 - MPI CHANNEL DISCONNECTED
- Event 15 - H323 CALL SETUP
- Event 16 - H323 CLEAR INDICATION
- Event 24 - SIP CALL SETUP
- Event 25 - SIP CLEAR INDICATION
- Event 27 - RECORDING SYSTEM LINK
- Event 110 - OPERATOR ON HOLD PARTY
- Event 113 - CONFERENCE REMARKS
- Event 2108 - OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 1
- Event 3001 - CONFERENCE START CONTINUE 2
- Event 3108 - OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 2
- Event 4001 - CONFERENCE START CONTINUE 3
- Event 4108 - OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 3

Appendix D

Ad Hoc Conferencing

The *Polycom RMX 1800* Ad Hoc conferencing feature enables participants to start ongoing conferences on-the-fly, without prior definition when dialing an Ad Hoc-enabled Entry Queue. The created conference parameters are taken from the Profile assigned to the Ad Hoc-enabled Entry Queue.

Ad Hoc Conferencing

A participant dials in to an Ad Hoc-enabled Entry Queue and starts a new conference based on the Profile assigned to the Entry Queue. In this configuration, any participant connecting to the Entry Queue can start a new conference, and no security mechanism is applied. This mode is usually used in organizations where Ad Hoc conferences are started from within the network and without security breach.

A conference is started using one of the following method:

1   The participant dials in to the Ad Hoc-enabled Entry Queue.

2   The Conference ID is requested by the system.

3   The participant inputs a Conference ID via his/her endpoint remote control using DTMF codes.

4   The MCU checks whether a conference with the same Conference ID is running on the MCU. If there is such a conference, the participant is moved to that conference. If there is no ongoing conference with that Conference ID, the system creates a new conference, based on the Profile assigned to the Entry Queue, and connects this participant as the conference chairperson.
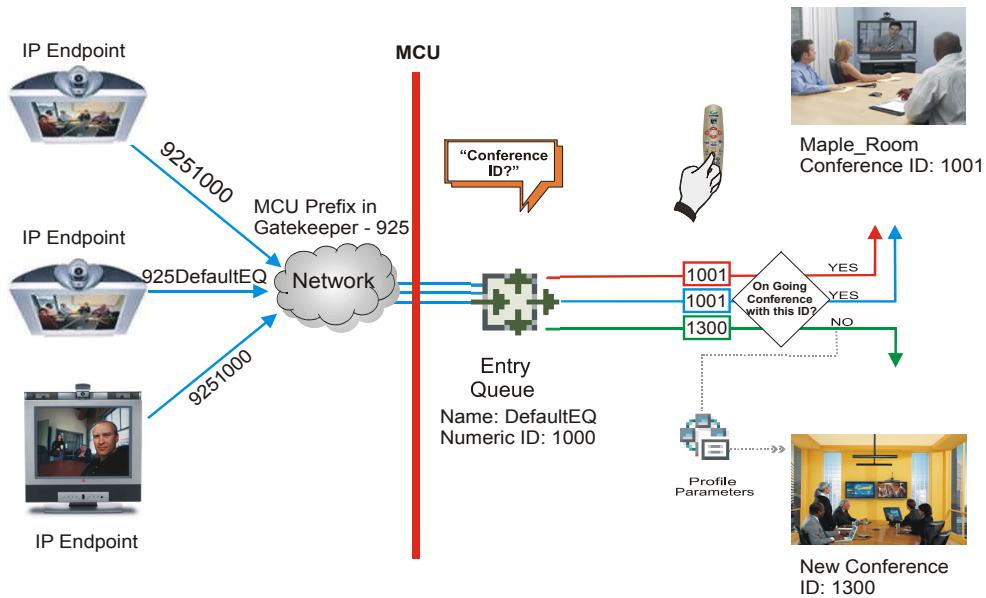
Figure D-1 *Ad Hoc Conference Initiation without Authentication*

To enable this workflow, the following components must be defined in the system:

- An Entry Queue IVR Service with the appropriate audio file requesting the Conference ID
- An Ad Hoc-enabled Entry Queue with an assigned Profile

System Settings for Ad Hoc Conferencing

Ad Hoc Settings

Before a participant can initiate an Ad Hoc conference, the following components must be defined:

- **Profiles**

  Defines the conference parameters for the conferences that will be initiated from the Ad Hoc-enabled Entry Queue. For more details, see *"Conference Profiles"* on page **2-1**.

- **Entry Queue IVR Service with Conference ID Request Enabled**

  The Entry Queue Service is used to route participants to their destination conferences, or create a new conference with this ID. For details, see *"IVR Services"* on page **15-1**.

  In Ad Hoc conferencing, the Conference ID is used to check whether the destination conference is already running on the MCU and if not, to start a new conference using this ID.

- **Ad Hoc - enabled Entry Queue**

  Ad Hoc conferencing must be enabled in the Entry Queue and a Profile must be assigned to the Entry Queue. In addition, an Entry Queue IVR Service supporting conference ID request. For details, see *"Entry Queues"* on page **7-1**..

Appendix E

Participant Properties Advanced Channel Information

The following appendix details the properties connected with information about audio and video parameters, as well as, problems with the network which can affect the audio and video quality.

Table E-1 Participant Properties - Channel Status Advanced Parameters

Field	Description
Media Info	
Algorithm	Indicates the audio or video algorithm and protocol.
Frame per packet (audio only)	The number of audio frames per packet that are transferred between the MCU and the endpoint. If the actual Frame per Packets are higher than Frame per Packets declared during the capabilities exchange, a Faulty flag is displayed.
Resolution (video only)	Indicates the video resolution in use. If the actual resolution is higher than resolution declared in the capabilities exchange, the Faulty flag is displayed. For example, if the declared resolution is CIF and the actual resolution is 4CIF, the Faulty flag is displayed.
Frame Rate (video only)	The number of video frames per second that are transferred between the MCU and the endpoint.
Annexes (video only)	Indicates the H.263 annexes in use at the time of the last RTCP report. If the actual annexes used are other than the declared annexes in the capabilities exchange, the Faulty flag is displayed.
Channel Index	For Polycom Internal use only.

Table E-1 Participant Properties - Channel Status Advanced Parameters (Continued)

Field	Description
RTP Statistics	
Actual loss	The number of missing packets counted by the IP card as reported in the last RTP Statistics report. If a packet that was considered lost arrives later, it is deducted from the packet loss count. Packet loss is displayed with the following details: • ***Accumulated N*** - number of lost packets accumulated since the channel opened. • ***Accumulated %*** - percentage of lost packets out of the total number of packets transmitted since the channel opened. • ***Interval N*** - number of packets lost in the last RTP report interval (default interval is 5 minutes). • ***Interval %*** - percentage of lost packets out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). • ***Peak*** - the highest number of lost packets in a report interval from the beginning of the channel's life span.
Out of Order	The number of packets arriving out of order. The following details are displayed: • ***Accumulated N*** - total number of packets that arrived out of order since the channel opened. • ***Accumulated %*** - percentage of packets that arrived out of order out of the total number of packets transmitted since the channel opened. • ***Interval N*** - number of packets that arrived out of order in the last RTP report interval (default interval is 5 minutes). • ***Interval %*** - percentage of packets that arrived out of order out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). • ***Peak*** - the highest number of packets that arrived out of order in a report interval from the beginning of the channel's life span.

Table E-1 *Participant Properties - Channel Status Advanced Parameters (Continued)*

Field	Description
Fragmented	Indicates the number of packets that arrived to the IP card fragmented (i.e., a single packet broken by the network into multiple packets). This value can indicate the delay and reordering of fragmented packets that require additional processing, but is not considered a fault. The Fragmented information is displayed with the following details: • **Accumulated N** - total number of packets that were fragmented since the channel opened. • **Accumulated %** - percentage of fragmented packets out of the total number of packets transmitted since the channel opened. • **Interval N** - number of fragmented packets received in the last RTP report interval (default interval is 5 minutes). • **Interval %** - percentage of fragmented packets out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). • **Peak** - the highest number of fragmented packets in a report interval from the beginning of the channel's life span.

Appendix F

Configuring Direct Connections to the Collaboration Server

Direct connection to the Collaboration Server is necessary if you want to:

- Modify the Collaboration Server's *Factory Default Management Network* settings without using the USB memory stick.
- Connect to the Collaboration Server's *Alternate Management Network* for support purposes.
- Connect to the Collaboration Server via a modem.

Management Network (Primary)

If you do not want to use the USB memory stick method of modifying the Collaboration Server's *Management Network* parameters, it is necessary to establish a direct connection between a workstation and the Collaboration Server.

Configuring the Workstation

The following procedures show how to modify the workstation's networking parameters using the *Windows New Connection Wizard*.

For non-Windows operating systems an equivalent procedure must be performed by the system administrator.

Before connecting directly, you must modify the *IP Address*, *Subnet Mask* and *Default Gateway* settings of the workstation to be compatible with either the Collaboration Server's *Default Management Network* or *Alternate Management Network*.

To modify the workstation's IP addresses:

1 On the Windows *Start* menu, select **Settings > Network Connections.**

2 In the *Network Connections* window, double-click the **Local Area Connection** that has *Connected* status.
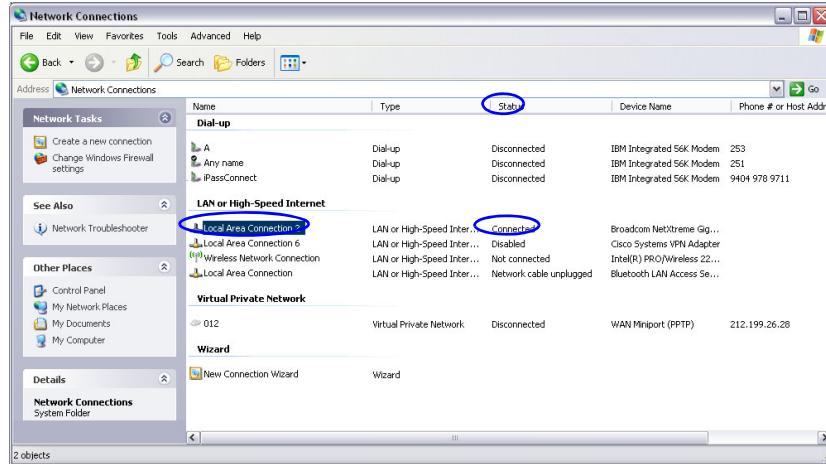
3 In the *Local Area Connection Status* dialog box, click the **Properties** button.
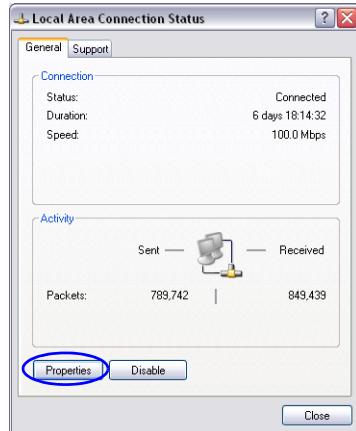

4 In the *Local Area Connection Properties* dialog box, select **Internet Protocol [TCP/IP] > Properties**.
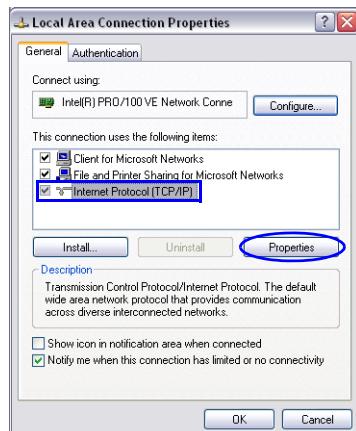
5 In the *Internet Protocol (TCP/IP) Properties* dialog box, select **Use the following IP address**.

6 Enter the *IP address, Subnet mask* and *Default gateway* for the workstation.
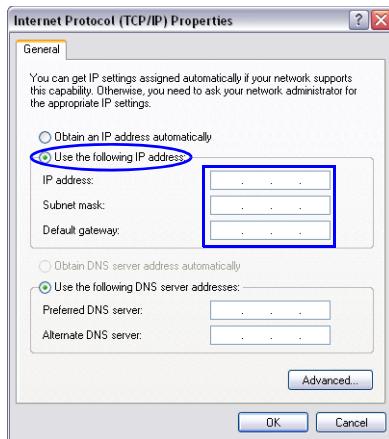
The workstation's IP address should be in the same network neighborhood as the Collaboration Server's *Control Unit* IP address.

Example: *IP address* – near **192.168.1.nn**

> None of the reserved IP addresses listed in *Table F-1* should be used for the IP Address.

The *Subnet mask* and *Default gateway* addresses should be the same as those for the Collaboration Server's *Management Network*.

The addresses needed for connection to either the Collaboration Server's *Default Management Network* or *Alternate Management Network* are listed in Table F-1.

For more information about connecting to the *Alternate Management Network*, see "*Configuring Direct Connections to the Collaboration Server*" on page **F-1**.

Table F-1   Reserved IP Addresses

| Network Entity	IP Address	
	Management Network (Factory Default)	Alternate Network
Control Unit IP Address	192.168.1.254	169.254.192.10
Control Unit Subnet Mask	255.255.255.0	255.255.240.0
Default Router IP Address	192.168.1.1	169.254.192.1

7 Click the **OK** button.

Connecting to the Management Network

To connect directly to the Collaboration Server:

1 Connect the power cable and power the Collaboration Server **On**.

2 Start the *Collaboration Server Web Client* application on the workstation, by entering the factory setting *Management IP* address in the browser's address line and pressing **Enter**.

3 In the *Collaboration Server Web Client* Login screen, enter the default *Username* (**POLYCOM**) and *Password* (**POLYCOM**) and click the **Login** button.

The *Fast Configuration Wizard* starts.
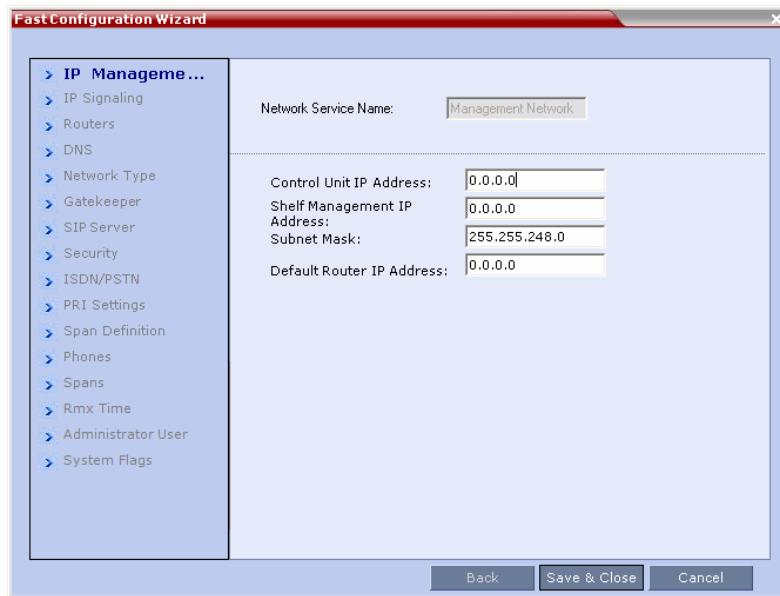
If no *USB memory stick* is detected and **either**: this is the *First Time Power-up* **or** the *Default IP Service* has been deleted and the Collaboration Server has been reset, the following dialog box is displayed:

For more information about First-time Power-up and the *Fast Configuration Wizard* see the *Polycom RMX 1800 Getting Started Guide*, *"Procedure 1: First-time Power-up"* on page **2-8**.

4 Enter the following parameters using the information supplied by your network administrator:

— *Control Unit IP Address*
— *Shelf Management IP Address*
— *Control Unit Subnet Mask*
— *Default Router IP Address*

5 Click the **Save & Close** button.

The system prompts you to sign in with the new *Control Unit IP Address.*

6 Disconnect the LAN cable between the workstation and the LAN Port on the Collaboration Server's back panel.

7 Connect LAN Port on the Collaboration Server's back panel to the local network using a LAN cable.

8 Enter the new *Control Unit IP Address* in the browser's address line, using a workstation on the local network, and press **Enter** to start the *Collaboration Server Web Client* application.

9 In the *Collaboration Server Web Client* Login screen, enter the default *Username* (**POLYCOM**) and *Password* (**POLYCOM**) and click the **Login** button.

Remote access to the Collaboration Server's *Alternate Management Network* is supported via an external PSTN <=> IP modem.

Appendix G

SIP RFC Support

Table G-1 *SIP RFC Support in RealPresence Collaboration Server (RMX) Systems*

SIP RFC	Description	Note
1321	MD5	
2032	RTP Payload for H.261	
2205	RSVP	
2327	Session Description Protocol (SDP)	
2429	RTP Payload for H.263+	
2833	RTP Payload for DTMF	
2617	HTTP Authentication	
2976	SIP Info Method	
3261	SIP	
3264	Offer/Answer Model	
3265	SIP Specific Event Notification	Limited support
3311	SIP Update Method	
3515	SIP Refer Method	Limited support
3550	RTP	
3551	RTP Profile for Audio/Video	
3711	SRTP	
3890	Transport Independent Bandwidth Modifier for SDP	
3891	SIP Replaces header	Limited support
3892	SIP Referred-by Mechanism	Limited support
3984	RTP Payload format for H.264	
4028	Session Timers in SIP	
4145	TCP Media Transport in SDP	
4566	Session Description Protocol (SDP)	

Table G-1 *SIP RFC Support in RealPresence Collaboration Server (RMX) Systems (Continued)*

SIP RFC	Description	Note
4568	SDP Security Descriptions	
4573	H.224 RTP Payload (FECC)	
4574	SDP Label Attribute	
4582	Binary Floor Control Protocol (BFCP)	
4583	SDP for BFCP	
4796	SDP Content Attribute	
5168	XML Schema for Media Control (Fast Update)	
cc-transfer	Call Transfer Capabilities in SIP	Limited support